STATE OF MINNESOTA

IN SUPREME COURT

No. C4-85-1848

In re: Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch

---

Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch

FINAL REPORT

June 28, 2004

Hon. Paul H. Anderson, chair

Mark R. Anfinson, Mpls.
Donna Bergsgaard, Eagan
Van Brostrom, Hastings
Sue K. Dosal, St. Paul
Hon. Kathleen R. Gearin, St. Paul
Donald A. Gemberling, St. Paul
Paul R. Hannah, St. Paul
Hon. Natalie Hudson, St. Paul
Hon. Timothy J. McManus, Hastings
Gene Merriam, St. Paul
Jane F. Morrow, Anoka
Teresa Nelson, St. Paul
Pamela McCabe, Anoka
Hon. John R. Rodenberg, New Ulm
Hon. Warren Sagstuen, Mpls.
Robert Sykora, Mpls.
Lolita Ulloa, Mpls.
Gary A. Weissman, Mpls.

Michael B. Johnson, St. Paul
Staff Attorney

Susan J. Larson, Esq., Milbank, South Dakota
Consultant

SJI This report was developed in part under grant number SJI-03-T-063 from the State Justice Institute. The points of view expressed are those of the committee and do not necessarily represent the official position or policies of the State Justice Institute.

Table of Contents

Acknowledgements

The advisory committee would like to thank the many individuals who participated in this project and assisted in our efforts to broadly reach out to all who may be affected by court record access policy. In particular the committee thanks those who submitted written and oral comments in response to the committee's preliminary recommendations. All of these contributions were crucial to the committee's work and will also benefit the Supreme Court as it reviews the committee's recommendations.

The committee would also like to thank the State Justice Institute for its generous support through a technical assistance grant that helped to provide the type of staff support necessary to this project. The committee is also grateful to Alan Carlson of the Justice Management Institute and Martha Wade Steketee of the National Center for State Courts for providing the committee with extensive insight into the development of the report entitled *Public Access to Court Records: Guidelines for Policy Development by State Courts*, prepared by the Conference of Chief Justices and Conference of State Court Administrators.

Finally, the committee would like to thank its dedicated staff, including Michael Johnson and Susan Larson for their research and writing, and Kristina Ford and Kathy Zajac for their administrative and editorial assistance. The committee is also grateful for the assistance of the information technology staff who provided technical expertise and assistance, including Darrel Austin, Nancy Crandal, Dale Good, Robert Hanson, Pete McNair, Eric Stumne, and Jim Wehri.

Recommendations on Rules of Public Access to Records of the Judicial Branch

Introduction

By order dated January 23, 2003, the Minnesota Supreme Court established an advisory committee to review, and make recommendations concerning, the RULES OF PUBLIC ACCESS TO RECORDS OF THE JUDICIAL BRANCH ("ACCESS RULES"). The Supreme Court directed the advisory committee to consider, among other things, the report entitled *Public Access to Court Records: Guidelines for Policy Development by State Courts*, prepared by the Conference of Chief Justices and Conference of State Court Administrators ("*CCJ/COSCA Guidelines*").[1]

The *CCJ/COSCA Guidelines* reflect a growing national debate[2] over whether and to what extent court records should be accessible electronically. Among the many issues that the *CCJ/COSCA Guidelines* were designed to address were: which records should be published on the Internet and what privacy protections are necessary; what databases should be accessible in whole or in part to the public; and what fees, if any, should be charged.

The *CCJ/COSCA Guidelines* provide a starting point and framework for analysis; they do NOT establish a single, proposed national standard on electronic access issues. The advisory committee used this framework to assist in its review of the ACCESS RULES. Consistent with both the *CCJ/COSCA Guidelines* and the Court's practice when it appointed the predecessor committee in 1986, the advisory committee includes representatives from several areas affected by access policy.[3]

The advisory committee met sixteen times after its establishment. In addition to discussing the information access experiences and interests of its members, the committee received presentations from:

- the *CCJ/COSCA Guidelines* staff and co-chair regarding development of the *CCJ/COSCA Guidelines* and issues addressed therein;
- a commercial data broker (West, a Thomson company) regarding its use of court records;

---

[1] The *CCJ/COSCA Guidelines* are posted at http://www.courtaccess.org/modelpolicy/.

[2] *See, e.g.*, Jennifer Lee, *Dirty Laundry, Online for All to See*, N.Y. Times, September 5, 2002.

[3] A detailed roster is attached as Exhibit F to this report.

- the director of the Privacy Rights Clearinghouse regarding identity theft and other privacy interests; and
- the leading executive branch data access expert (Donald Gemberling) regarding executive branch data access law and policies, and the fair information principles[4] incorporated in those laws and policies.

The advisory committee was also fortunate to obtain a small grant from the State Justice Institute to assist the committee in collecting, organizing and reviewing materials, especially the developments in other state and federal courts regarding electronic access to court records.[5] The committee also solicited the advice of the Supreme Court Implementation Committee on Multicultural Diversity and Fairness in the Courts, and the Supreme Court Technology Planning Committee's Data Policy Subcommittee, which subcommittee has been reviewing the *CCJ/COSCA Guidelines* and addressing access to records issues in the court technology area.

The advisory committee also solicited general public comment in response to a preliminary report that was posted on the main state court web page, and invited commentators to address the committee at a public hearing. Many witnesses testified at the hearing, including representatives of the clergy, the print and electronic media, various community groups, citizens, public defenders, court reporters, and judges. A complete list of the hearing witnesses is attached in Exhibit O, appended to this report. A summary of the testimony and other written comments received is attached as Exhibits P and Q. The full comments are posted under the Public Notices section of the main state court web page (www.courts.state.mn.us).

The advisory committee reviewed its recommendations in response to the comments received at the public hearing. Attached as exhibits to this report are

---

[4] See http://privacy.med.miami.edu/glossary/xd_fair_info_principles.htm; see also Gemberling, Weissman, *Data Practices at the Cusp of the Millennium*, 22 WM. MITCHELL L. REV. 767 (1996). The fair information principles are also discussed in Exhibit H: Minority Report: Fair Information Principles, attached to this report. The minority report ignores the fundamental differences between executive branch and judicial branch functions, and fails to recognize that court procedure already incorporates fundamental fairness.

[5] Websites tracking these developments are maintained by the National Center for State Courts at http://www.courtaccess.org, the Reporters Committee for Freedom of the Press at http://rcfp.org/courtaccess/viewstates.cgi, and the Center for Democracy and Technology at http://www.cdt.org/publications/020821courtrecords.shtml#mn.

final proposed changes to the ACCESS RULES and various other court rules addressing public access to court records. The text of this report and the advisory committee comments to the attached rules describe the proposed changes.

The report also contains minority and plurality reports on several issues. Although advisory committee members did not have an opportunity to articulate responses to all of these reports, committee members were advised that they may submit additional comments at the hearing before the Supreme Court.

Internet Access

Introduction.

Historically, court records in paper format have been broadly accessible to any member of the public willing to travel to the courthouse. The policy reasons for such access include promoting public trust and confidence in the courts and providing public information and education about the results of cases and the evidence supporting them. Access to court records is becoming easier and much broader now that an electronic format replaces or augments the traditional paper format. The Internet's capacity to consolidate information into easily searchable databases means that the trip to the courthouse is a virtual journey accomplished with the click of a computer mouse. These changes have eroded the practical obscurity[6] that individuals identified in court records once enjoyed, and requires a

[6] Before the transition to electronic court records began, it was impractical for anyone to build significant dossiers on individuals from publicly accessible paper records because the number of potential sources was too great and the volume of information was unwieldy. This became known as "practical obscurity." *See*, e.g., *U.S. Dept. of Justice v. Reporters Committee for the Freedom of the Press*, 489 U.S. 749, 109 S.Ct. 1568 (1989) (public access to the Federal Bureau of Investigation's national clearinghouse of arrest and conviction information was an unwarranted invasion of personal privacy under public access exceptions to the Federal Freedom of Information Act). Despite the Supreme Court's recognition of this privacy interest in compiled government information, some advisory committee members believe that practical obscurity is an illusion or at the least it is eroding, and that private data brokers will continue to collect court information in paper if remote access is not available, and then resell the data on the Internet. Some commentators believe that practical obscurity is a problem to be solved, not a virtue (public hearing written comments of John Borger, Star Tribune), that it does not apply to primary source records such as court records, and that many people who weigh in on the issue are not fully aware of the level of access that exists now (public hearing comments of Prof. Jane Kirtley, Silha Center for Study of Media Ethics and Law, School of Journalism & Mass Communication, University of Minnesota).

Some advisory committee members counter that there is a difference between using private sector resources to compile and resell public information and using taxpayer dollars to do the same thing. Some commentators believe that the court's imprimatur, its tremendous power and trust, give its records commercial value (public hearing comments of John Stuart, State Public Defender), and that this

(footnote continued next page)

review of access policies to ensure that a proper balance is maintained between many competing and often conflicting interests including, but not limited to, protection against unsubstantiated allegations, identity theft protection, accuracy, public safety, accountability of courts and government agencies, victim protection and efficiency.

For example, solutions designed to avoid discriminatory impact on persons of color make it more difficult for society to become aware of certain root problems. Publishing unproven criminal accusations on the Internet, discussed in more detail in another section of this report, can result in the denial of housing and job opportunities especially for persons of color who are disproportionately represented in cases where such accusations are ultimately dismissed. Not making the information available on the Internet, however, makes it more difficult for society to become aware of the disproportionate number of dismissals and its root causes, and to address them.

Similar conflicting interests affect crime victims. Most crime victims prefer to minimize Internet access to victim identifiers and locators (e.g., name, address, etc.), because such access has the potential of leading to more victimization and

---

(footnote continued from previous page)
distinguishes court records from other government records such as law enforcement records (public hearing comments of Don Samuels, Minneapolis City Council Member). Other committee members also point out that the Minnesota Legislature also sought to protect personal privacy in statewide compilations, and such protections continue, for example, to prohibit public access to executive branch statewide compilations of arrest and corrections monitoring information. Although in 1993 the legislature began to allow public access to statewide adult felony, gross misdemeanor and targeted misdemeanor conviction information maintained by the Minnesota Bureau of Criminal Apprehension ("BCA") for a period of 15 years following discharge of the sentence (1993 MINN. LAWS ch. 171, § 2; codified as MINN. STAT. § 13.87, subd. 1), statewide arrest information maintained by the BCA continues to be private (Minn. Stat. § 13.87, subd. 1 (2002)), while arrest data in the hands of the originating law enforcement agency remains public. MINN. STAT. § 13.82 (2002). Portions of the Department of Corrections' Statewide Supervision System ("SSS") involving the monitoring and enforcing of conditions of release remain off limits to the public under MINN. STAT. §§ 241.065; 299C.147 (2002), while portions of the SSS relating to statewide booking and detention, which were formerly maintained in the Department's separate Detention Information System, remain accessible to the public despite being merged with the SSS. MINN. DEPT. ADMIN. ADVISORY OPINION 03-041 (Oct. 1, 2003).

revictimization through intimidation and embarrassment, while nothing positive is gained from publishing victim identifiers and locators on the Internet. Victims may also benefit from some public access to location information, however, such as being able to document that a particular neighborhood has a high incidence of crimes.

Similarly, solutions supporting the prevention of identity theft[7] conflict with the goal of accuracy. One approach to counter identity theft is to minimize the amount of personal identifying information about individuals, such as social security numbers, dates of birth, addresses, telephone numbers, etc., that is conveniently accessible to the public from electronic court records. The less identifying information that is available, however, the greater the likelihood that individuals will be misidentified as having been the subject of certain court records such as money judgments or criminal convictions.[8] Such inaccuracies can have far reaching consequences.

---

[7] The advisory committee sought the advice of privacy experts and was advised that identity theft is a crime of opportunity, wide-open remote access to court records provides significant opportunity for such theft to occur, and identity theft makes life miserable for its victims. Presentation by Beth Givens, Director, Privacy Rights Clearinghouse, to Advisory Committee (July 27, 2003; power point). Some committee members disagree and believe that privacy concerns are exaggerated and are based on speculation and anecdotes, and that privacy invasions resulting from court record disclosures are rare. The Dissenting Statement set forth in Exhibit L, for example, argues that the 2003 Federal Trade Commission report, *Identity Theft Survey Report*, suggests that electronic access to public records is not a major contributor to this crime. Similar industry surveys also show that, of the victims who know how the perpetrator obtained their personal information, only a very small amount say the source was public records. *See, e.g.*, Privacy and American Business Survey Finds 33.4 Million Americans Victims of ID Theft (July 30, 2003; press release). In the Privacy and American Business Survey, however, the vast majority of the respondents (approximately 80%) did not know how their personal information was obtained, and in the FTC Survey half of the victims did not know how their information was obtained.

[8] The Consumer Data Industry Association submitted written comments to the committee indicating that access to the full social security number is the only way to correctly match records with the correct consumer. Letter from Eric Ellman, Director and Counsel, Government Relations, Consumer Data Industry Association, to Michael Johnson, advisory committee staff, undated. See also the Dissenting Statement set forth in Exhibit L.

Some uses of court records may cause harm. It is impossible to distinguish between valid requests for information and those requests that may cause harm. Some potential harm can be minimized by legislative activity, such as fair credit reporting laws[9] that require consumer reporting agencies and their data suppliers to verify and correct public record information. In addition, potential harm must be balanced with potential benefits, such as the ability to screen potential employees/workers and keep government accountable.

Many times in emotional proceedings such as family court matters, domestic abuse matters and other civil suits very personal and private information is disclosed. Allegations are made in these proceedings through affidavits which many times relay abusive, inappropriate or dysfunctional behavior between the parties and their children. For example, it is necessary for a domestic abuse victim to give specific facts regarding the abusive actions of his or her[10] partner. A parent must also be specific regarding abuse and neglect when making a motion for a change in custody. Access to this information by anyone at any time can create further embarrassment, harassment and victimization of the parties. Unsubstantiated allegations of abusive or inappropriate behavior also raise significant concerns. The overwhelming majority of petitioners in domestic abuse Order For Protection[11] and other Harassment restraining order[12] proceedings are representing themselves. A growing number of family court motions are also being handled without an attorney. Unrepresented litigants do not have the same ethical duties as a lawyer in such situations.[13] Internet publication of nonmeritorious allegations can harm a person's reputation even if a final court order finds that the allegations are without merit. Those who really need access

---

[9] Federal Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*., as amended by the Fair Accurate Credit Transactions Act of 2003, Pub. L. 108-159, and the Minnesota consumer reports law, MINN. STAT. § 13C.001 *et seq*. (2003).

[10] Studies indicate that the majority of abuse victims are women. *See, e.g.*, U.S. DEPT. OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, BUREAU OF JUSTICE STATISTICS, INTIMATE PARTNER VIOLENCE, 1993-2001 (2003) (1,247 women and 440 men were killed by an intimate partner in 2001).

[11] MINN. STAT. § 518B.01 (2002).

[12] MINN. STAT. § 609.748 (Supp. 2003).

[13] *Compare* MINN. R. CIV. P. 11.02 (requires objective reasonableness under the circumstances; applicable to both attorneys and unrepresented parties; sanctions cannot be imposed until after notice and a reasonable opportunity to respond) *with* MINN. R. PROF. CONDUCT 3.1, 3.3 (lawyer's duties regarding meritorious claims and candor towards the tribunal). Historically, courts have been more reluctant to award sanctions against unrepresented litigants. *Liedtke v. Fillenworth*, 372 N.W.2d 50, 52 (Minn. App. 1985).

for a legitimate purpose (such as the media reporting on the development of a case) can obtain the information from the courthouse. Internet publication of allegations made in these types of actions can harm a person's reputation even if a final court order finds that the allegations are without merit.[14]

Alternative Approaches.

The advisory committee looked at several approaches in its attempt to resolve these policy issues: One approach is to simply allow Internet access to all court records that are accessible to the public in paper format, and make any necessary adjustments to both paper and Internet records. Another approach is to try to retain the same level of public access to paper records and publish only a limited number of those records on the Internet.

Proponents of the first approach believe that: (1) requiring a person to come to the courthouse to get information that is available to the public is not meaningful access but is a restriction of the public's legitimate use of information that is otherwise easily available in electronic format, and thus the second approach is on shaky legal ground; (2) if there is a valid public use for a certain record in paper format, it should be available on the Internet as well; (3) it is unrealistic to conclude that in the future the courts can have all their files in electronic format but only provide paper-based access at the courthouse; (4) where access is limited to the courthouse, commercial data brokers will harvest the information anyway and will make it available, and it will only be available to those who can afford to pay a broker's fee; (5) accuracy will only be improved by putting the records on the Internet and exposing problems; (6) there are enormous benefits to remote access to court records, including reducing burdens on court staff, improving the accuracy and timeliness of news reporting, ensuring public safety and national security, and minimizing risks to financial institutions; (7) redacting is feasible using current technology; (8) trying to solve social problems by keeping information off of the Internet is not good public policy; (9) the solution for misuse is for the legislature to prohibit the misuse and for the executive branch to vigorously enforce those laws; and (10) courts in Maryland, New York, and the federal system have adopted wide open Internet access policies and no

[14] Internet publication of allegations prior to a decision on the merits by a court compounds the injury that a false allegation can cause. As discussed over the next several sections of the report, advisory committee members have conflicting views on whether such publication serves valid public policy.

demonstrable harm has come from it, just like Minnesota's experience with recent changes that opened child protection court records to public access.[15]

Those favoring limited Internet publication of records believe that: (1) there is a difference between "public" records and "publishing" records on the Internet; (2) publication of only certain records on the Internet is an expansion of existing public access at the courthouse and not a limitation on public access at all; (3) limited information should be placed on the Internet only after procedures and rules are in place to protect privacy interests; (4) just because technology enabling Internet access is available does not mean that it should be used for all matters; (5) if the first approach is taken (i.e., allowing all public, paper records to be published on the Internet), there will be a backlash of public opinion that will likely sweep broad categories of information completely out of public view; (6) relying on legislation prohibiting misuse and vigorous enforcement of those laws is itself illusory; (7) the public currently has a good understanding of what is going on in the courts without adding more Internet access; and (8) similar data accessible through commercial data brokers and even other government entities, such as law enforcement) does not carry the imprimatur of the court.[16]

Those favoring limited Internet publication of records also cite that: (1) after 18 months of study, the *CCJ/COSCA Guidelines* Committee concluded that there is a difference between "public" and "publishing" court records on the Internet; and (2) some courts that have broadly published records on the Internet have had to pull back and reconsider their policy in light of privacy concerns raised by persons identified in the records.[17]

---

[15] *See, e.g.*, public hearing comments of Lucy Dalglish, Reporters Committee for Freedom of the Press, et al,; public hearing comments of Chris Ison and John Borger, Star Tribune; public hearing comments of Prof. Jane Kirtley, Silha Center for Study of Media Ethics and Law, School of Journalism & Mass Communication, University of Minnesota; public hearing comments of Gary Hill, KSTP-TV et al.; and written comments of Eric Ellman, Consumer Data Industry Association. *See also* attached Exhibits K and L (minority reports discussing benefits of full Internet access and balancing of interests).

[16] *See, e.g.*, public hearing comments of John Stuart, State Public Defender; public hearing comments of Kizzy Johnson, Communities Against Police Brutality; public hearing comments of Scott Benson and Don Samuels, Minneapolis City Council Members.

[17] For example, the clerk of court in Butler County, Ohio, was ordered to turn off Internet access to court records until domestic relations cases could be removed due to concerns over disclosure of social security numbers, bank account numbers and other personal information. See Janice Morse, *Separating Court Records for*

(footnote continued next page)

Some proponents of full Internet publication indicate that they could support limited Internet publication primarily because it is likely there will be a backlash to the first approach. Thus, the committee is proceeding with the approach of attempting to retain the same level of public access to paper records and publish only a limited number of those records on the Internet.

Deciding What to Publish on the Internet.

Several advisory committee members believe that the courts should publish information on the Internet only for a variety of public purposes, including: the most effective use of court and court staff; customer service; supporting the role of, and public trust and confidence in, the judiciary; promoting government accountability; contributing to public safety; and minimizing risk of injury to individuals (including protecting privacy rights and proprietary business information).

The advisory committee also believes it is important to consider the fiscal impact that access policies have. Redacting sensitive information from often voluminous documents prepared and filed by the parties to a case creates administrative burdens and liability exposure for court staff, although immunity and technology such as XML tagging may eventually minimize this burden. Making some information available on the Internet will save court administration staff time, but staff and possibly judge time spent responding to complaints may also increase depending on what is published on the Internet. If the underlying information is public on paper, the information likely will be available from private sector data brokers. Currently much information is available for a fee through a commercial data broker service. Those persons without funds, however, may not have such access.

(footnote continued from previous page)
Net Access May Be Costly, Cincinnati Enquirer, July 24, 2003. The clerk of court in Loudon County, Virginia, unplugged his subscription-based remote access service after concerns over disclosure of personal information caused the county board to formally request the action and the creation of a task force to study the issue. See *Clemens Unplugs Online Remote Access System*, Leesburg2Day, 7/24/03. Even the federal judicial conference had to back away from its initial Internet access for criminal records. See *Federal Judges, Agencies Block Online Access to Public Records*, Associated Press, 10/12/01 (citing access by inmates who harassed or beat other inmates, and access to presentence investigation reports which contain sensitive material).

Personal Identifiers

There was nearly unanimous agreement by the advisory committee that some information deserves privacy protection, such as social security numbers, financial account numbers, telephone numbers, and street addresses of litigants, jurors, witnesses and victims of criminal and delinquent acts. To achieve this kind of protection, the judicial system needs a process for redacting private information before publishing the records on the Internet. The committee believes that this result is practical only if remote access is limited to documents that the courts themselves generate, such as the register of actions, calendars, judgment dockets, and judgments, orders, appellate opinions, and notices prepared by the court.[18] The committee's recommendation on Internet access to case records is set forth in proposed ACCESS RULE 8, subd. 2 (set forth in Exhibit A attached to this report).

The advisory committee believes, however, that there should be an exception to this recommendation to allow for the type of high volume public access requests that come with high profile cases. The Fourth Judicial District, for example, recently posted all trial exhibits from the *Gordon et al v. Microsoft* case on its web site. When as in this case there are hundreds of exhibits, such posting clearly reduces an otherwise significant administrative burden of responding to requests for copies of the documents. The committee believes that it should trust the discretion of the presiding judge to decide on a case-by-case basis whether Internet posting of exhibits and/or other documents prepared or submitted by the parties is appropriate. Existing procedure, including appellate review, provides parties with the opportunity to be heard in the decision making process. The exception is included in the proposed rule.

Some judicial districts already publish court calendars on the Internet. Internet access to the register of actions (i.e., name, index, list of activities occurring on the case) would provide greater access and would eliminate the need for individuals

[18] Some commentators argue that: (1) while SSN and financial identifiers may implicate legitimate privacy concerns, home addresses and telephone numbers do not; (2) precluding Internet access to witness, juror, and victim identifiers is excessive; (3) access to identifiers is critical to allow reporters to track down and interview participants and report stories of clear interest to the public; and party-filed documents contain the most useful information for understanding a case and that limiting access to these because of concerns over social security numbers is excessive. Public hearing comments of Prof. Jane Kirtley, Silha Center for Study of Media Ethics and Law, School of Journalism & Mass Communication, University of Minnesota; public hearing comments of Lucy Dalglish, Reporters Committee for Freedom of the Press, et al..

and certain companies to travel to the courthouse and use courthouse space and equipment to obtain information.

Judgments, orders, and notices prepared by the court have integrity in that they are the product of an adjudicatory process. The same may not be true of other documents. For example, while an affidavit filed by a party may truthfully reflect that a particular allegation has been made, the affidavit does not have the same integrity.[19] In addition, the courts control the issuance of judgments, orders and notices. The burden of not including certain items for Internet publication should not unduly interfere with the preparation of these items. If a social security number or victim's name needs to be included in a particular judgment or order, the court has the opportunity to prepare a publicly accessible paper version and an Internet accessible version without too much additional effort. The advisory committee realizes that its proposal to allow Internet access to all case records that the courts themselves generate will require education of judges, attorneys and court staff in order to avoid exposing the judicial branch to significant liability or the type of criticism that undermines the public trust and confidence in the courts.

Several advisory committee members reminded the committee that it needs to consider all perspectives, including that of the poor, minorities,[20] victims, jurors and witnesses. The committee learned that most victims of crime prefer that all victim identifiers (name, address, telephone numbers, etc.) not be published on the Internet because such access will lead to more victimization and re-victimization. Some committee members believe that if the courts have to sacrifice protection of victims, jurors and witnesses in order to implement Internet access, then the courts simply should not implement Internet access. A majority of the committee agreed that victim, juror and witness identifiers should not be accessible through the limited, court-generated records that the committee believes should be accessible on the Internet.

Unproven Criminal Allegations

The issue that received the most attention during the public hearing was whether the courts should publish unproven criminal allegations on the Internet. There are racial and social implications that pull at both sides of the issue.

---

[19] Author and Yale Law Professor Stephen L. Carter draws a distinction between truth and integrity in his article, *The Insufficiency of Honesty* (Atlantic Monthly, Feb. 1996, p.74-76) (reproduced at http://www.csun.edu/~hfmgt001/honesty.doc).

[20] Some court records now are not accessible to all citizens due to language barriers, but they are available with the help of an interpreter.

Impact on Communities of Color

Over a decade ago the Minnesota Supreme Court Racial Bias Task Force found that people of color were arrested more often, charged more often, required to post higher bails, and given longer sentences, than whites.[21] Unfortunately, these trends appear to continue.

According to the results of a study conducted in 2001 by the Minneapolis-based Council on Crime and Justice, African American drivers are stopped by police at a rate much greater than their presence in the population.[22] Once stopped, African Americans generally are more likely to be arrested than white people.[23] And once they have made it through the court system, the ratio of African Americans to whites in state prison is about 25 to 1. This is the highest ratio of all states.[24] In 2000, 37.2% of the state's prisoners were African American. By comparison only 3.5% of the population of Minnesota was African American.[25]

Charges against African Americans also result in a disproportionate number of dismissals. In 2001 the Council on Crime and Justice studied 2600 arrests in the city of Minneapolis for six low level offenses: driving after revocation, driving after suspension, driving without a license, loitering with intent to commit prostitution or to sell narcotics, and lurking with intent to commit a crime.[26] The study found that 78% of defendants arrested and booked were also charged (i.e., ended up in court records), but only 20% were convicted. Of those charged, 33% had no criminal history, and 10% had been arrested at least once before without

---

[21] *Minnesota Supreme Court Task Force on Racial Bias on the Court System Final Report*, May 1993, at S-5, S-9, and S-19. Some judges and attorneys surveyed by the task force felt that the race of the defendant and victim play a role in sentencing in Minnesota. *Id*., at S-12. The task force also found that persons of color often chose not to go to trial because of the perception that they would not receive a fair trial. *Id*. At S-15.

[22] In a study of Minneapolis police stops, African American drivers accounted for 37% of vehicle stops despite comprising only 18% of the population. Thomas L. Johnson, Cheryl Widder Heilman, *An Embarrassment to All Minnesotans: Racial Disparity in the Criminal Justice System*, Bench & Bar of Minnesota (May/June 2001).

[23] *Id*. In Minneapolis, African Americans were found to be about two and one half times more likely to be arrested and booked than whites following a traffic stop; Native Americans about three times more likely.

[24] *See*: http://www.crimeandjustice.org/Pages/Projects/RDI/RDI%20Reports.htm

[25] *Id*.

[26] Public hearing comments of Tom Johnson, Council on Crime and Justice.

any conviction ever having been obtained. A disproportionate percentage of those arrested (74%) and those charged (79%) were African American, but only 18% were convicted. Many more African Americans had multiple previous arrests without convictions than whites; 86% of those having more than five arrests without convictions were African American.

Other sources corroborate the high number of dismissals. For example, the state public defender's office handles approximately 175,000 cases annually, and 15,000 of these result in outright dismissals (i.e., they are not the result of plea bargains or not guilty verdicts).[27] Minneapolis accounted for 11,000 of the dismissals, with 10,000 dismissed by the prosecutor. In the vast majority of these dismissals (95%), the charges were not screened by a prosecutor before they were filed with the court (either as tickets or tab charges). Once filed with the court, however, the defendant's name and charge appear on the courts' records including court calendars.

Based on these statistics and anecdotal information the advisory committee received comments from many community leaders and groups who propose that no preconviction court records be published via the Internet. These proponents are deeply concerned that making preconviction court records available to anyone at any time and in virtual perpetuity over the Internet will have a permanent, disproportionate impact on the housing and employment of persons of color, especially young men of color.[28] Proponents of keeping preconviction records off the Internet point out that while judges and lawyers can distinguish between a charge and a conviction, such important distinctions are not made by the general public or in the world of housing and employment.[29]

---

[27] Public hearing comments of John Stuart, State Public Defender.

[28] Public hearing comments of Archbishop Harry J. Flynn, Archdiocese of St. Paul and Minneapolis; public hearing comments of public hearing comments of Tom Johnson, Council on Crime and Justice; Pastor Albert Gallmon, Jr. Fellowship Missionary Baptist Church, Minneapolis; public hearing comments of Hon. George Stephenson, District Court, Second Judicial District; public hearing comments of Roger Banks, State Council on Black Minnesotans; public hearing comments of Kizzy Johnson, Communities Against Police Brutality; public hearing comments of Don Samuels, Minneapolis City Council Member; public hearing testimony of Bishop Craig E. Johnson, Evangelical Lutheran Church in America, Minneapolis Area Synod.

[29] Public hearing comments of Archbishop Harry J. Flynn, Archdiocese of St. Paul and Minneapolis; public hearing comments of Gordon Stewart, Legal Rights Center.

Proponents of keeping preconviction records off the Internet also argue that publishing preconviction court records on the Internet: (1) will undermine the efforts of the Court's Implementation Committee on Multicultural Diversity and Fairness in the Courts;[30] (2) will degrade the presumption of innocence which the courts have a constitutional duty to protect; (3) will shame and marginalize the innocent instead of protecting them; (4) will increase our racial and class divide rather then narrow it; (5) will make the court a part of the wider web of injustices that it seeks to eliminate; (6) is both immoral and un-American; and (7) is unnecessary for public interest research purposes as many data sources currently exist to support public interest research.[31]

When it was pointed out by advisory committee members that cities currently sell arrest information in bulk to commercial data brokers who in turn sell the information through subscription services, and that some jails post their current list of detainees on the Internet, these proponents countered that: (1) two wrongs do not make a right; (2) law enforcement data lacks the imprimatur of the court; (3) law enforcement data is only available from local offices while statewide compilations of such records are accorded privacy by statute; (4) aside from jail detainees and special projects, cities are not posting arrest information on the Internet.[32]

While recognizing that relatively few overall criminal cases involve the falsely or mistakenly accused, proponents of keeping preconviction records off the Internet stress the impact that Internet publication can have, particularly for people of

---

[30] The Implementation Committee unanimously supports the proposal that no preconviction court records be published via the Internet. See March 17, 2004, Minutes, Implementation Committee on Multicultural Diversity and Fairness in the Courts, at p. 1.

[31] Public hearing comments of Archbishop Harry J. Flynn, Archdiocese of St. Paul and Minneapolis; public hearing comments of Pastor Albert Gallmon, Jr. Fellowship Missionary Baptist Church, Minneapolis; public hearing comments of Hon. George Stephenson, District Court, Second Judicial District; public hearing comments of Gordon Stewart, Legal Rights Center; public hearing comments of Roger Banks, State Council on Black Minnesotans; public hearing comments of Kizzy Johnson, Communities Against Police Brutality; public hearing comments of Don Samuels, Minneapolis City Council Member; public hearing comments of Scott Benson, Minneapolis City Council Member; public hearing testimony of Bishop Craig E. Johnson, Evangelical Lutheran Church in America, Minneapolis Area Synod.

[32] Public hearing comments of John Stuart, State Public Defender; public hearing comments of Don Samuels, Minneapolis City Council Member.

color. One commentator remarked "it is easy for some in our society to say 'If you really wanted to work, you could find a job,' or 'that's what happens when you commit a crime.' Those who have said so are less likely to have found themselves unemployed and/or homeless lately."[33]

Response to Impact on Communities of Color

The advisory committee also heard from various groups, mostly media representatives, opposed to any limits on Internet publication of preconviction court records. These opponents point out that: (1) even where there are demonstrable cases of Internet access to court records causing injury to reputation, this is not sufficient to overcome the presumption of public access;[34] (2) the high number of dismissals is a problem that should be reported;[35] (3) trying to solve social problems by keeping information off of the Internet is poor public policy, our system of government operates best when it is open to public scrutiny;[36] (4) if misuse of records is a genuine threat, then it is the legislature's job, not the court's, to define and take steps to prevent illegal acts;[37] (5) the less access there is to court records, the less accurate, fair and timely news reporting will be because news is a 24 hour business and courthouses have limited hours;[38] (6) dire predictions about the awful consequences of public access were made to the Minnesota Supreme Court prior to its recent decision to allow more public access to child protection cases, but a lengthy experimental period produced no evidence showing that those predictions were warranted;[39] and (7) by keeping court records off the Internet, the public will know less about the courts and public perception of the courts will suffer.[40]

A few advisory committee members noted that Internet access to unproven criminal charges through the court's registers of actions will also serve the goal of holding law enforcement accountable for the use of its arrest and detention

[33] Public hearing comments of the Hon. George Stephenson, District Court, Second Judicial District.
[34] Public hearing comments of Lucy Dalglish, Reporters Committee for Freedom of the Press, et al.
[35] *Id.*
[36] Public hearing comments of Prof. Jane Kirtley, Silha Center for Study of Media Ethics and Law, School of Journalism & Mass Communication, University of Minnesota.
[37] *Id*.
[38] Public hearing comments of Chris Ison, Editor, Star Tribune.
[39] Public hearing comments of Gary Hill, KSTP-TV et al.
[40] *Id.*

authority, and also the goals of holding the prosecutor and the courts accountable for their role in such matters. Such access can benefit defendants by providing the information necessary to expose shortcomings in the criminal justice system. Public safety is also served by knowledge of who has been charged with a crime. The relatively few overall criminal cases involving the falsely or mistakenly charged simply do not outweigh the significant benefits of Internet access.[41]

Using Technology to Minimize Automated Harvesting

Some advisory committee members see a distinction between an individualized need for public access to court records over the Internet and a commercial need for such access. Thus, the committee considered technology that would attempt to make preconviction court records accessible in some way via the Internet, but less susceptible to automated harvesting by commercial data brokers. This approach attempts to preserve some level of practical obscurity for preconviction records and yet provide a means for some convenient public access.

Many of Minnesota's judicial districts post calendars on the Internet, and these calendars contain both preconviction and postconviction records. These calendars permit the public to see what is transpiring in their courts. A combination of random, non-predictable file names for the calendars plus nontext, image only format, plus a "prove-you-are-human log-in procedure" between each calendar file request theoretically can prevent automated searching devices from simply harvesting preconviction records by name from these calendars displayed on the Internet while permitting individual public access.

An example of the prove-you-are-human log-in procedure is referred to as a "Turing test" named after British mathematician Alan Touring. The "test" consists of a small distorted picture of a word and if the viewer can correctly type in the word, access or log in to the system is granted. Right now, software programs do not read clearly enough to identify such pictures. Theoretically, this will separate the human reader from the automated software program that is designed to simply harvest data on a particular individual.

The format of court calendars is also important. Most calendars are produced in a PDF format readable through common and freely available software (Adobe Acrobat Reader). The PDF format can be either a text searchable format or an

[41] See attached Exhibits K and L (minority reports discussing benefits of full Internet access).

image only graphic format. The effort required to search an image-only format by name is certainly greater than that for text-based format.

Use of random and nonpredictable file names is necessary to reduce the possibility of avoiding the log-in process and jumping directly to the calendar file. Otherwise, if the Monday calendar file is always titled "Mondaycalendar," then software programs will know what file to look for.

Names indexes present a particular problem in the preconviction context. Most court case management systems include both name and case number indexes to locate the cases. Removing the name index completely is one option, but that also removes the name index from postconviction matters as well. Another option is to remove the preconviction cases from the reach of the name index search.

The advisory committee was concerned about the potential ramifications of these measures, both in terms of effectiveness and overall costs and in terms of impact on the courts' current technology efforts, including the roll out of its new case management system known as MNCIS. Also of concern was the impact on current customers of electronic records in the Fourth Judicial District, which publishes conciliation court, housing court, and high-profile case records over the Internet, and has in excess of 200 paid subscribers to its electronic access service that includes all of its civil and criminal case records. The committee appointed a special fact-finding subcommittee to investigate the potential ramifications, and the results of that subcommittee's work is attached as Exhibit N to this report.

The fact-finding subcommittee found that these measures would not significantly affect the budget or time frame for the MNCIS project. The advisory committee will have to define "preconviction" with enough detail to allow IT staff to correctly implement any policy.

The impact on the Fourth Judicial District is less clear, although its separate SIP system will eventually be replaced by MNCIS within the next year, which may obviate most of the problem. Taking away preconviction records from subscription customers may add staff and terminal equipment and operation costs as it is anticipated that current subscribers will continue to obtain preconviction records by coming to the courthouse.

Regarding continued effectiveness, court technology staff has advised the advisory committee that there is no real yardstick. Technological advances may eventually obviate any of these measures, but advances and vigilance may also provide new measures and continued effectiveness. It is anticipated that keeping ahead of technical advances will be a constant struggle.

Recommendation on Unproven Criminal Accusations

By a close vote of 9 to 7, a majority of the advisory committee agreed that Internet publication of preconviction court records should, to the extent feasible, be posted on the Internet in a format that is not searchable by defendant name by automated tools. This means that preconviction cases can appear on court calendars posted on the Internet if measures are taken to prevent automated searching, such as using prove-you-are-human log-ins, random file names, and image-only file format. This also means that a criminal case in preconviction status will not show up on a name index search conducted via the Internet but will show up on a name index search conducted at the courthouse public access terminal. This recommendation is codified in proposed Rule 8, subd. 3(c).

The recommendation defines "preconviction" criminal case records as records for which there is no conviction as defined in MINN. STAT. § 609.02, subd. 5 (2003), which states:

> "Conviction" means any of the following accepted and recorded by the court:
>
> (1) a plea of guilty; or
> (2) a verdict of guilty by a jury or a finding of guilty by the court.

The Minnesota Supreme Court has ruled that the general practice to be followed is to have a conviction "recorded" in a judgment entered in the file in accordance with MINN. R. CRIM. P. 27.03, subd. 7.[42] That rule states:

> "Subd. 7. Judgment. The clerk's record of a judgment of conviction shall contain the plea, the verdict of findings, and the adjudication and sentence. If the defendant is found not guilty or for any other reason is entitled to be discharged, judgment shall be entered accordingly. The sentence or stay of imposition of sentence is an adjudication of guilt

Thus, a continuance for dismissal under MINN. STAT. § 609.132 that occurs before any guilty plea is accepted and "recorded" by the court as provided above would not be a conviction. Similarly, any diversion that occurs before a guilty plea is accepted and "recorded" by the court as set forth above would not be a conviction. A stay of imposition or execution of sentence, on the other hand, constitutes an

[42] *State v. Hoelzel*, 639 N.W.2d 605 (Minn. 2002).

adjudication under MINN. R. CRIM. P. 27.03, subd. 7, quoted above, and a conviction would be considered "recorded" once the record of a judgment has been entered in the file.[43] Other situations that would not result in a "recorded" conviction include the retention of unadjudicated offenses under MINN. STAT § 609.04 (2003) or issuing a stay of adjudication under *State v. Krotzer*, 548 N.W.2d 252 (Minn. 1996).[44]

Attorney Records

Information on licensed and registered attorneys is maintained by the Clerk of the Appellate Courts in the attorney registration database. Rule 9 of the Rules of the Supreme Court for Registration of Attorneys limits public access to attorney information both over the Internet and in bulk record disclosures:

> Rule 9. ACCESS TO ATTORNEY REGISTRATION RECORDS
> Attorney registration records shall be accessible only as provided in this rule.
>
> A. Public Inquiry Concerning Specific Attorney. Upon inquiry, the Clerk of the Appellate Courts may disclose to the public the name, address, admission date, continuing legal education category, current status, and license number of a registered attorney, provided that each inquiry and disclosure is limited to a single registered attorney.
> B. Publicly Available List. The Clerk may also disclose to the public a complete list of the name, city, and zip code of all registered attorneys.
> C. Lists Available to Continuing Legal Education Providers and the Courts. Upon written request and payment of the required fee, the Clerk may disclose to a bona fide continuing legal education business a complete list of the name, address, admission date, continuing legal education category, current status, and license number of all registered attorneys. The Clerk may also disclose the same information to a court or judicial district solely for use in updating mailing addresses of attorneys to be included in a judicial evaluation program.

---

[43] The fact that a person may eventually complete probation without the sentence being imposed or executed merely affects the level of conviction rendered. *See* MINN. STAT. §§ 609.13, .135 (2003).

[44] *State v. Hoelzel, supra.*

D. Trust Account Information. Trust account information submitted by attorneys as part of the attorney registration process is not accessible to the public except as provided in the Rules of Lawyer Trust Account Board. Rules of the Supreme Court for Registration of Attorneys

This rule was developed after consultation with members of the bar and attorney information is now available on the main court web site (www.courts.state.mn.us). The attorney registration database feeds information into court case record management systems at all levels. Thus, the same limitations on access to attorney information will apply to the attorney registration information imported into case management systems.

Conviction Records

One advisory committee member believes that there is no need for the courts to "publish" criminal conviction information on the Internet in light of the publication of conviction information by the Minnesota Bureau of Criminal Apprehension ("BCA"),[45] and in light of the fact that the court is bound to ensure that dissemination of conviction information does not obviate the rehabilitative goals of the criminal justice system. Other committee members noted, however, that the BCA makes publicly accessible only felony, gross misdemeanor, and targeted misdemeanor conviction information for a period of 15 years after discharge from sentence,[46] and that records that the BCA cannot match with fingerprint files are not publicly accessible. These committee members also pointed out that conviction information is necessary for background checks on all potential tenants and employees (not just those for whom statutes mandate a background check). Thus, there is a need for court publication of conviction records.

Family Law Records

A small number of the advisory committee believes that: (1) the details of marriage dissolution (except the fact that marriage dissolution occurred and the dissolution's impact on real estate) are "nobody's business" and that the requirement for court intervention to rescind a marriage contract should not

[45] The BCA is required to provide Internet access to this information by July 1, 2004, and may charge a fee for such access. MINN. STAT. § 13.87, subd. 3 (Supp. 2003).
[46] MINN. STAT. § 13.87, subd. 1 (2002).

change what is essentially private business into a public matter; (2) traditional appellate remedies and freedom of speech are sufficient means to keep judges accountable so further accountability through public access is not necessary; and (3) access to Internet and paper records of marriage dissolution cases should be limited to a certificate of dissolution and a summary real estate title document.[47] Most other committee members, however, believe that limiting Internet access to court-controlled records, coupled with expanded closure of financial source documents discussed above, removes a significant amount of troublesome information from public access and that some public access is necessary to hold the court system accountable in marriage dissolution cases.

Go Slow Approach Recommended

The advisory committee's recommendations on Internet access[48] should be viewed as the first step in a go-slow approach to providing more remote access to information. As indicated above, some courts that have simply begun posting all public records on the Internet have encountered numerous problems and have had to pull back and reconsider their policy in light of privacy concerns raised by persons identified in the records. The committee agreed that the potential for damage to individuals necessitates a careful approach.

Bulk Records

Bulk records refer to compiled records such as a database containing some or all of the elements of an online computer system. The courts have historically maintained such databases for analytical purposes, and the advent of data warehouse technology makes the data more accessible.

Deciding What Records to Release in Bulk

In its January 2004 preliminary report for public comment, the advisory committee recommended that only those court records that are accessible to the public on the Internet (discussed above) should be accessible to the public in bulk format.[49]

---

[47] See Minority Report-Family Law Records, set forth in Exhibit G attached to this report.

[48] See proposed ACCESS RULE 8, subd. 2, set forth in Exhibit A attached to this report.

[49] Supreme Court Advisory Committee on the Rules of Public Access to Records of the Judicial Branch, *Preliminary Recommendations of the Supreme Court Advisory Committee on the Rules of Public Access to Records of the Judicial Branch, Report for Public Comment,* Jan. 21, 2004, p. 12. The report also (footnote continued next page)

Near the end of its deliberations, the committee adopted this recommendation by a vote of 11-3. At the final meeting, a proposal to modify the recommendation was presented. After it was pointed out that a member of the minority could not make a motion to reconsider the issue, the proposal failed because no motion was made. All committee votes, however, were taken subject to review of the final draft of the report, which was to include all minority reports members desired to submit. At the end of the review period, a minority report recommending the modified bulk data proposal was submitted together with information indicating that a number of committee members now supported the modified bulk data proposal. Not all members had an opportunity to review or comment on the modified bulk data report before the end of the review period. In order to maintain the integrity of the committee process and allow clear expression of the level of committee support for the various alternative proposals, the alternative proposals on bulk data access are set forth in the proposed rule as alternative drafts of ACCESS RULE 8, subd. 3. Each alternative and its level of committee support is explained in a separate exhibit attached to the report (see Exhibits I, J and K). Exhibit L also addresses the alternatives. The committee believes that it is appropriate and sufficient to note that the recommendation regarding what court records should be released in bulk format is contested and that the committee is closely divided on the issue.

Fees for Bulk Records

The advisory committee also discussed the fees to be charged for bulk data. Section 6.0 of the *CCJ/COSCA Guidelines* suggests that "reasonable fees" should be charged for bulk data. ACCESS RULE 8, subd. 3, currently allows a commercially reasonable fee for data with commercial value.[50] The State Court

---

(footnote continued from previous page)
included a minority recommendation that all court records publicly accessible in any format at the courthouse should be accessible in bulk format. *Id.* at p. 67.

[50] The current charge of 2.81 cents per-kilobyte is based on fees paid by on-line users in a pilot project that involves agency access to the state courts' TCIS® system from which the database is extracted. Each TCIS® screen contains between 1,000 and 2,000 characters, and in 1993 when the rate was first set there were approximately 33 million transactions. With an operating budget of approximately $5.5 million dollars for that year, users paid on the average 16.9 cents per 1.5 kilobyte of data. If it is assumed that there are four potential customers of the extract data (two newspapers, one TV station, and at least one commercial firm), the allocated costs would be 2.81 cents per kilobyte of data.
(footnote continued next page)

Administrator's Office currently charges by the kilobyte for bulk data, and waives all but the copy costs for media and educational and noncommercial scientific institutions whose primary purpose is scholarly or scientific research, as long as the recipients agree to sign a fee waiver agreement that restricts the use of the data to noncommercial purposes.

Some advisory committee members believe that the courts should sell bulk data at high fees and use the proceeds to balance budgets and pay for public defenders and computer system development. Other members, however, believe that: (1) bulk data will only be accessible to sophisticated, capital-backed groups and that the average person will not have any meaningful access to bulk data; (2) the implementation of new data warehouse tools might eventually allow the public to obtain reports online; and (3) commercial data brokers will continue to harvest case records on a case-by-case basis and market their own bulk and online systems.

(footnote continued from previous page)
Given that transactions and budgets have increased slightly since then, the 2.81 cents per kilobyte remains an appropriate fee.

The above charge is more than consistent with other state agency charges for data. The Department of Administration Print Communication Division charges $60.00 per 1,000 names and addresses for computer disk versions of mailing lists for licensed professionals (see htttp://www.comm.media.state.mn.us/bookstore/files/2003mlscatalog.pdf). A typical address contains approximately 100 to 200 characters or bytes. This yields a cost of between $.60 and $.30 per kilobyte (plus a flat $25 copy preparation cost). Moreover, most of these lists are maintained using off-the-shelf software, not sophisticated information systems like TCIS®.

The secretary of state offers numerous database tapes containing business registration information (names, addresses, tradenames, agent names, etc.). In 1993, when the court's 2.81 cents per kilobyte charge was established, the secretary of state's office "licensed" a complete set of 11 nine-track tapes containing all business records for $11,840. The tapes held a maximum of 18 megabytes each, which yielded a charge of $.05979 or $.06 per kilobyte. The license precludes the user from sublicensing the data and limits use to the normal course of the licensee's business. A license for the entire set now sells for $13,500, although the size has grown somewhat (pricing is not available online but only by calling 651-296-2803).

A majority of the advisory committee believes that bulk data should not be put on the Internet, but should be sold for commercial (i.e., revenue generating) fees. This fee recommendation is currently a part of the ACCESS RULES and is being renumbered as proposed ACCESS RULE 8, subd. 3 (see Exhibit A attached to this report). A minority of the committee believes that bulk data should be accessible on the Internet and that fees should be limited to actual costs of providing the data.[51]

Correcting Inaccuracies in Court Records

Another issue highlighted in the CCJ/COSCA Guidelines is the development of a policy on correction of inaccuracies in court records. Although inaccuracies have occurred from time to time in paper-format court records, the advent of Internet publication will significantly magnify the potential for harm that such errors can cause. Procedures have long existed for correcting paper-format records, and the advisory committee has recommended practical approaches to properly correct clerical errors in case records (see proposed ACCESS RULE 7, subd. 5).

There are some clerical or data entry-type errors that a court administrator can correct without the need for a court order. These include changes to the calendars and indexes. Changes to orders and judgments and other parts of the record, however, require formal legal action to correct.[52] The advisory committee is

---

[51] *See* Exhibit J.

[52] *See, e.g.*, MINN. GEN. R. PRAC. 375 (expedited child support process; clerical mistakes, typographical errors, and errors in mathematical calculations in orders …arising from oversight or omission may be corrected by the child support magistrate at any time upon the magistrate's own initiative or upon motion of a party after notice to all parties); MINN. R. CIV. P. 60.01 (civil cases; clerical mistakes in judgments, orders, or other parts of the record and errors therein arising from oversight or omission may be corrected by the court at any time on its own initiative or on the motion of any party, and after such notice, if any, as the court orders); MINN. R. CRIM. P. 27.03, subds. 8, 9 (criminal cases: clerical mistakes in judgments, orders, or other parts of the record or errors in the record arising from oversight or omission may be corrected by the court at any time and after such notice, if any, as the court orders; the court may at any time correct a sentence not authorized by law); MINN. R. JUV. PROT. P. 41.01 (juvenile protection cases; clerical mistakes in judgments, orders, or other parts of the record and errors arising from oversight or omission may be corrected by the court at any time upon its own initiative or upon motion of any party and after such notice, if any, as the court orders; during the pendency of an appeal, such mistakes can be corrected with leave of the appellate court); MINN. R. CIV. APP. P. 11.05
(footnote continued next page)

aware of errors such as the wrong address or even the wrong name recited in a criminal complaint. Such errors may surface during preliminary court hearings where corrections are conveniently made or authorized by the court. Such errors can also surface informally in a telephone call to court administrative staff who in turn may either point out the requirements for obtaining relief by motion or refer the matter to the source of the record (e.g., the prosecutor) who then takes appropriate steps to rectify the situation (e.g., a motion or corrected filing).

The advisory committee recommends a rule that allows a party to submit to the court administrator a written request for correction of court records along with evidence that the request has been served on all parties. The rule places a duty on court administrative staff to respond to a correction request by correcting the records when correction does not require an order, by forwarding a request for correction to the appropriate place (i.e., judge or a party), or by returning the request and allowing the individual to request other appropriate, formal relief from the court (e.g., in the form of a motion). The committee believes that a written request is not a significant barrier to non-English speaking individuals as it is no more difficult than filling out an application to proceed *in forma pauperis* (i.e., without payment of filing fees). Although service on parties is normally not involved in the *in forma pauperis* application situation (because the other party is often not involved in the litigation at that point), in many circumstances due process arguably requires notice to opposing parties when modifications to court records are sought.

It is still not clear what remedy is available when the individual affected by an inaccurate court case record is not (or was not) a party to the case. Only parties or others with standing (e.g., a guardian ad litem) can make motions to the court. The Minnesota Supreme Court has determined that intervention[53] is an appropriate process for nonparties to contest the closure of civil case records.[54] It is not clear whether intervention would be available for the purpose of correction of a civil case record,[55] and even if it were, it is not a very practical solution. It is also not

---

(footnote continued from previous page)
(differences as to whether the transcript or other parts of the record on appeal truly disclose what occurred in the trial court are to be submitted to and determined by the trial court; material omissions or misstatements may be resolved by the trial court, stipulation of the parties, or on motion to the appellate court).

[53] MINN. R. CIV. P. 24.

[54] *Minneapolis Star & Tribune v. Schumacher*, 392 N.W.2d 197 (Minn. 1986) (contesting closure of minor settlement records).

[55] MINN. R. CIV. P. 24.01 permits intervention as a matter of right when "the applicant claims an interest relating to the property or transaction which is the
(footnote continued next page)

clear how often the need for nonparty correction of court records will arise. The advisory committee's recommendations do not address this issue.

Changes Regarding Access to Case Records

The foregoing recommendations on Internet access, bulk access, and record correction represent the core of the advisory committee's work. The committee also considered whether there are court case records that should not be accessible to the public regardless of the format (i.e., paper or electronic). The commentary to Section 4.6 of the *CCJ/COSCA Guidelines* lists records that courts should consider making confidential whether in paper or electronic (i.e., Internet) format. The committee compared the items on this list with Minnesota law[56] and the law of several other jurisdictions, and considered comments and information received by the advisory committee. The committee is recommending only a few changes to existing law regarding public access to case record information in all formats.

Race Information

At the request of the Minnesota Supreme Court Implementation Committee on Multicultural Diversity and Racial Fairness in the Courts ("Implementation Committee"), the state trial courts have recently begun to collect race data from litigants in criminal, traffic, and all juvenile court matters. The litigants in these cases are asked to fill out a race census form[57] and the court staff then enters the race information into the trial courts' online computer systems.[58] The paper forms

---

(footnote continued from previous page)
subject of the action and the applicant is so situated that the disposition of the action may as a practical matter impair or impede the applicant's ability to protect that interest." MINN. R. CIV. P. 24.02 provides permissive intervention when "the applicant's claim or defense and the main action have a common question of law or fact."

[56] The State Court Administrator maintains tables of these laws and rules. The committee recommends that the periodically updated tables posted on the state court web site replace Appendices B, C and D under the current ACCESS RULES (see proposed Rules 4, 5 and 6 attached in Exhibit A to this report).

[57] The main census form is attached as Exhibit E to this report. A Spanish translation is also available.

[58] This is not the only type of race data contained in trial court computer systems. Other race data fields capture race data from other sources such as pleadings and reports filed in the cases. Some of these source documents are not accessible to the public, such as presentence investigation reports. MINN. STAT. §§ 609.115,
(footnote continued next page)

are not retained in the court files related to the case and are destroyed after the data is entered. Currently, race census data are not displayed on public access terminals attached to these online systems, but the race census data are included in the bulk data databases[59] that are provided to the public.[60]

The advisory committee solicited the opinion of the Implementation Committee as to whether public access to race census data should be: (1) completely prohibited expect by court order (which presumably would mean that some researchers might be permitted access by court order); (2) prohibited only when access is sought via the Internet; (3) wide open including Internet publication; or (4) some other variation.[61] The Implementation Committee unanimously believes that access to race census data should be completely prohibited in any form, whether via the Internet, courthouse terminal, or paper documents, except that the court may allow access for research purposes pursuant to court order that limits ultimate public disclosure of the research to aggregate statistics that do not identify individuals by their race.[62]

The Implementation Committee's rationale includes that:

- Public disclosure of race census data undermines public trust and confidence in the courts because it takes advantage of a litigant's vulnerability; most are willing to disclose their race status for use in obtaining fair results, but not for resale to others.
- The fact that race information may be accessible in some form in a court file (e.g., in a charging instrument or a police report), does not justify

---

(footnote continued from previous page)
subds. 4, 6; 609.2244 (2002). Once entered into the system, however, there is no means of determining which source document was used, and this commingling of inaccessible with potentially accessible information results in no public access to the race data entered in these other race data fields. The race data would, however, be accessible to the public through the source document when that document itself is accessible to the public.

[59] Data is extracted from the online systems and maintained in extract databases or data warehouses.

[60] Juvenile delinquency databases, for example, are not accessible to the public. MINN. STAT. §§ 260B.163, subd. 1; 260B.171, subd. 4 (2002); MINN. R. JUV. DEL. P. 30.

[61] The implementation committee also provided an opinion concerning remote access to preconviction criminal records, discussed earlier in the report.

[62] See March 17, 2004, Minutes, Implementation Committee on Multicultural Diversity and Fairness in the Courts, at p. 1

making all race data more accessible; this changes the court's role from adjudicator to compiler.

- Access to race census data for legitimate research purposes can be authorized pursuant to court order; the Minnesota Supreme Court has a longstanding tradition of making non-publicly accessible juvenile court records available for legitimate research purposes pursuant to a court order and accompanying nondisclosure agreement.[63]

The advisory committee learned that public access to other statewide repositories of race data varies. The Department of Public Safety's Criminal Justice Statistics Center (formerly known as Minnesota Planning), for example, provides the public with only aggregate statistical information that does not link race/ethnicity with an individual defendant.[64] The Minnesota Sentencing Guidelines Commission, however, regards its monitoring data as public and the data includes links between offender and his or her race/ethnicity.[65]

Some advisory committee members believe that public access to race census records must be limited in order to continue to obtain a sufficiently high response rate for the race census forms. In contrast, other committee members believe that public access should be unlimited because complete public scrutiny of race-related issues is necessary to maintain a fair system.[66] These committee members point out that the race census records currently are accessible to the public and that this has not deterred voluntary responses.[67] Opponents counter that the current race census form (set forth as Exhibit E to this report) provides no notice of potential public disclosure of an individual's race status, and implies that the information will only be used for ensuring a fair system.

By a one vote margin, the advisory committee recommends that race census records should not be accessible to the public in any form subject to one exception. The exception is that the records may be disclosed in bulk format pursuant to a nondisclosure agreement in which the recipient of the information agrees to disclose only aggregate statistical information that does not identify the

---

[63] *Id.*

[64] Email correspondence between Gail Carlson, Department of Public Safety, to Michael Johnson, advisory committee staff, dated March 18, 2004.

[65] Email correspondence from Jill Payne, Minnesota Sentencing Guidelines Commission, to Michael Johnson, advisory committee staff, dated March 18, 2004.

[66] *See, e.g.,* the minority attached as Exhibit M.

[67] *Id.*

race of any individual, and the custodian of the records reasonably determines that such access will not compromise the confidentiality of any individual's race. This is similar to what occurs now in regard to disclosure of juvenile court records for research purposes[68] except that only the nondisclosure agreement is required; the committee believes that there should be no need for a court order as long as an appropriate nondisclosure agreement is in place and the custodian of the records reasonably determines that such disclosure will not compromise the confidentiality of any individual's race status. The custodian's duty to make a reasonable determination that disclosure will not compromise the confidentiality of any individual's race status is taken from the "summary data" provisions of the executive branch Data Practices Act.[69] This recommendation is set forth in ACCESS RULE 4, subd. 1(e).

Juror Supplemental Questionnaires

In December 2001 the Minnesota Supreme Court Jury Task Force recommended that juror questionnaires used to supplement oral examination of jurors in civil

[68] Annual disclosures of juvenile delinquency records to the National Center for Juvenile Justice, for example, currently require a nondisclosure agreement between the Center and state court administration in which the Center agrees to limit disclosures to aggregate statistics, subject to attorney fees and injunctive relief for violations. Once the Agreement is signed, a request for disclosure is presented to the Supreme Court, which then issues an order authorizing disclosure of the records pursuant to the terms of the nondisclosure agreement. *See, e.g.*, *Order Authorizing Disclosure of Juvenile Court Database for Research Purposes*, No. C4-85-1848 (Minn. S. Ct. filed May 14, 2001).

[69] MINN. STAT. §§ 13.02, subd. 19; 13.05, subd.7 (2003). The minority report set forth in Exhibit L criticizes this approach in part on the basis that the person making the request must disclose their identity when they may wish to remain anonymous. The minority report then argues that preservation of anonymity is the reason the legislature expressly prohibits executive branch officials from demanding an identity as a condition of permitting access. MINN. STAT. § 13.03, subd. 12 (2002). What the minority left out is the fact that this applies only when the records are publicly accessible; a requestor's identity must be disclosed to an executive branch agency if the agency is going to allow the requestor access to confidential or private data for purposes of preparing "summary data." *See* MINN. STAT. § 13.05, subd. 7 (2002) (requestor must agree not to disclose and agency must reasonably determine that access by requestor will not compromise private or confidential data).

cases be sealed.[70] The advisory committee agrees with this recommendation (see proposed changes to MINN. R. CIV. P. 47.01, [71] attached as Exhibit B to this report). These supplemental questionnaires can contain highly personal information. Although the same issue exists in criminal cases, there are constitutional issues involved. The Minnesota Supreme Court has recently determined that individual answers to supplemental juror questionnaires in criminal cases may be sealed only after there has been a balancing of the juror's privacy interests, the defendant's right to a fair and public trial, and the public's interest in access to the courts. There must also be a finding that there is a substantial likelihood that conducting the voir dire in public would interfere with an overriding interest, including the defendant's interest in a fair trial and the juror's legitimate privacy interests in not disclosing deeply personal matters to the public.[72]

Juror Qualification Questionnaires and Social Security Numbers

A qualification questionnaire is forwarded to all individuals being called for jury service to obtain certain qualification information. Public access to the qualification information is governed by MINN. GEN. R. PRAC. 814, which delays unlimited public access until one year has elapsed since preparation of the list of jurors selected to serve and all persons selected to serve have been discharged. Prior to the expiration of the one-year period, the public may obtain access by submitting a written request with a supporting affidavit setting forth reasons for the request, and the court must grant the request unless the court determines that access should be limited in the interests of justice.

Although a few advisory committee members questioned the rationale for the one-year period in MINN. GEN. R. PRAC. 814, the committee concluded that no substantive change was needed at least in regard to civil cases. In regard to criminal cases, as the discussion above on supplemental questionnaires indicates, there are constitutional limitations. The criminal rules advisory committee has recommended that the "interests of justice" standard for closure of qualification questionnaire information during the one-year period be replaced with the standard and procedure applicable to supplemental juror questionnaires discussed above. In other words, public access to qualification questionnaires of jurors assigned to a

[70] *Minnesota Supreme Court Jury Task Force Final Report*, December 20, 2001, No. C7-00-100, at 32.

[71] MINN. GEN. R. PRAC. 814 governs qualification questionnaires that are mailed to jurors before they are summoned for jury service; but that rule does not apply to "supplemental" questionnaires which judges distribute to potential jurors.

[72] MINN. R. CRIM. P. 26.02, subd. 4(4) (effective 2-1-04).

criminal case could be limited only after there has been a balancing of the juror's privacy interests, the defendant's right to a fair and public trial, and the public's interest in access to the courts. Before limiting public access, the court must also make a finding that there is a substantial likelihood that conducting the voir dire in public would interfere with an overriding interest, including the defendant's interest in a fair trial and the juror's legitimate privacy interests in not disclosing deeply personal matters to the public. The access to records advisory committee agrees with this recommendation and the proposed changes to MINN. GEN. R. PRAC. 814 are set forth in Exhibit C along with other editorial and grammatical changes.

Another advisory committee recommendation affecting juror qualification information is to make explicit the requirement that juror social security numbers not be disclosed to the public or the parties in a case. This recommendation is also included in the proposed changes to MINN. GEN. R. PRAC. 814 attached as Exhibit C to this report. Social security numbers are required in order to pay juror fees in excess of a certain amount and there is no valid reason for disclosing the social security numbers beyond those involved in the fee payment process. Although current federal law combined with state requirements protects juror social security numbers, the federal law is difficult to understand[73] and jurors deserve a clear directive, particularly in light of recent criminal procedure modifications regarding access to juror information discussed in the preceding section of this report.

MINN. GEN. R. PRAC. 814 also addresses retention of juror records, and both the Minnesota Supreme Court Jury Task Force[74] and the Minnesota Supreme Court Advisory Committee on the rules of Criminal Procedure have made recommendations about the appropriate retention period. The Minnesota Supreme Court has assigned the issue of retention of jury records (along with other related administrative matters) to the to the Advisory Committee on the General Rules of

[73] 42 U.S.C. § 405(c)(2)(C)(viii) (2003).

[74] *Minnesota Supreme Court Jury Task Force Final Report*, December 20, 2001, No. C7-00-100, at 30; Supreme Court Advisory Committee on the Rules of Criminal Procedure, *Report and Proposed Amendments to the Rules of Criminal Procedure Concerning the Supreme Court Jury Task Force's Recommendations*, September 29, 2003, No. C1-84-2137, at pp. 6 and 7; Letter from Hon. Robert H. Lynn, Chair of the Criminal Rules Advisory Committee, to the Advisory Committee on Rules of Public Access, undated (clarifying position on retention issue).

Practice,[75] and the Access to Records Advisory Committee has not made a recommendation on this issue. Any comments received on the retention issue will be forwarded to the Advisory Committee on the General Rules of Practice for its consideration.

Party Social Security Numbers and Financial Documents

The advisory committee also recommended a change with respect to the treatment of social security numbers and financial information submitted in marriage dissolution cases. Current law and court rules direct parties to submit the social security number on a separate, confidential information sheet, and to submit tax returns in a confidential envelope. The ultimate responsibility for failure to redact the social security numbers currently lies with the court administrator. Such redaction is time consuming, and, in a file with numerous documents, the possibility of missing the redacting of just one social security number is great. The committee believes that it is appropriate to place the redaction burden on the persons who submit the documents to the court.[76] With the increasing number of unrepresented litigants in family law cases, however, the committee understands and recommends that this burden must be accompanied by clear education of litigants involved in these cases. The committee also agreed that financial account numbers and other financial source documents such as wage stubs, credit card statements and check registers should also be protected. The recommended procedures are set forth in proposed MINN. GEN. R. PRAC. 103, 313, and 355.05 and accompanying forms (attached as Exhibit D to this report).

Employer Identification Number

Closely related to the social security number of individuals is the federal employer identification number assigned to business entities. Although the executive branch

[75] *See Promulgation of Amendments to the Rules of Criminal Procedure*, No. C1-84-2137 (Minn. S.Ct. filed Dec. 10, 2003) (order promulgating rules and assigning issues).

[76] Federal law imposes the confidentiality of SSN whenever submission of the SSN is "required" by state or federal law enacted on or after October 1, 1990. 42 U.S.C. § 405(c)(2)(C)(viii) (2003). The committee proposes a rule whereby submission of SSN by the parties is only "required" when done in conformity with the rule. This approach has been successfully operating in the State of Washington. WASH. R. GEN. GR 22 (2003).

has a universal confidentiality requirement for social security numbers,[77] there is no similar blanket confidentiality for employer identification numbers. The employer identification number is confidential as part of tax return information in the hands of the state revenue and tax department,[78] and as part of independent contractor identification and payment information when vendors contract with executive branch agencies.[79] Although widespread access to a business' employer identification number may not raise the same identity theft risks as access to an individual's social security number, there is still some potential for mischief. The advisory committee has included in its recommendation some optional language that would protect the employer identification number from public access in case records to the same extent that the social security number is protected. The committee is particularly interested in obtaining feedback on this element of its proposals.

Witness Identifiers

A minority of the advisory committee believes that some witness identifiers such as addresses and telephone numbers should be kept out of public view entirely. Public access to witness identities does promote accountability. The majority of the committee believes that existing procedures for closing individual records remains an appropriate solution to address certain individual situations. Historically, dating back to the English tradition, the identity of witnesses assisted the community in determining the honesty of a witness. This may be particularly important in the case of expert witnesses whose opinions can be important to the outcome of cases.

Court Reporter Notes and Tapes

The Minnesota Association of Verbatim Reporters & Captioners ("MAVRC") association asked the advisory committee to consider modifying ACCESS RULE 3, subd. 5, as follows (additions indicated by underlined text):

> Subd. 5. "Records" means any recorded information that is collected, created, received, maintained, or disseminated by a court or court

[77] MINN. STAT. § 13.49 (2002) (does not apply to social security numbers filed in documents or records filed or recorded with the county recorder or registrar of titles, other than documents filed under section 600.13).
[78] MINN. STAT. § 270B.02, subd. 1 (2002).
[79] MINN. STAT. § 13.43 (2002); see also MINN. STAT. § 270.66, subd. 3 (2002) (requiring all persons doing business with the state of Minnesota to provide their social security number or employer identification number).

> administrator, regardless of physical form or method of storage. A "record" does not necessarily constitute an entire file, as a file may contain several "records." Court reporters' notes shall be available to the court for the preparation of a transcript when the court reporter is unavailable to produce a transcript in a timely manner. Court reporter's notes shall be defined as, in the case of stenographic court reporters, the court reporter's paper notes, and in the case of electronic reporters, the electronic reporter's tape recordings and logs.[80]

The purpose for the recommended change is to avoid public access to a stenographic reporter's backup tapes, which MAVRC believes are not a reliable method for capturing the record by themselves, and to ensure that the reporter who prepared the notes has an opportunity to transcribe them before the court turns them over to another reporter for transcription.[81] The Minnesota Supreme Court has recently modified the requirements for mandatory transcripts in both criminal and juvenile cases and, in doing so, has assigned to the General Rules of Practice Advisory Committee the responsibility for rule drafting regarding the availability of notes, tapes and personal dictionaries to the court for preparation of a transcript. The Access to Records Advisory Committee agrees that the ACCESS RULES should be limited to public access issues and that access by the court is appropriately the subject of some other set of rules, such as the general rules of practice for the district court.

Regarding public access to backup tapes, the proposed language would not achieve the result desired by MAVRC, i.e., precluding public access. The existing language in ACCESS RULE 3, subd. 5, regarding availability of notes to the court was clearly not intended to create any limitation on public access.[82] Thus, notes

---

[80] Letter from Barbara Nelson, President, Minnesota Association of Verbatim Court Reporters & Captioners, to Hon. Paul Anderson, advisory committee chair, dated February 9, 2004.

[81] *Id.*

[82] The predecessor advisory committee explained in its 1987 report that: (1) the term "record" would include a court reporter's stenographic notes that have been filed with a court administrator; (2) that freelance reporters often claimed that they own stenographic notes and refused to file them with the court notwithstanding the directive in Minn. Stat. § 486.03 for such filing; and (3) the committee concluded that it could not resolve the ownership issue within the ACCESS RULES but felt that it would be useful to clarify a court reporter's responsibility to make the notes available for preparation of a transcript. *Report to the Minnesota Supreme Court*
(footnote continued next page)

and backup tapes are subject to the general presumption of public access in ACCESS RULE 2 unless some other provision of law requires otherwise.

The state court administrator's office has consistently taken the position that: (1) conciliation court audio tapes are not accessible to the public under to ACCESS RULE 4, subd.1 (c) because the tapes only serve as the judge's notes as no official transcript can be made for these proceedings; (2) videotaped records of court proceedings are not accessible to the public under Minnesota Supreme Court order;[83] and (3) other tapes and notes are presumptively accessible to public provided the proceeding itself is accessible to the public, but the public may not have a copy of the tapes unless public audio or video coverage of the proceeding was authorized by court order.[84]

A few committee members are concerned that public access to backup tapes may result in no backup tapes being made. Beyond this, however, there was no support for a change to make all such tapes off limits to the public.

Administrative Records

The ACCESS RULES also address administrative records. These are records not related to specific cases, including employee records, law library records, and competitive bidding records. The advisory committee recommends changes designed to bring some of these provisions more in line with their executive branch counterparts, where appropriate (see proposed ACCESS RULE 5 set forth in Exhibit A to this report). Proposed committee comments following each rule explain the nature of the changes.

(footnote continued from previous page)
From the Advisory Committee on the Rules Governing Access to Records of the Judiciary, Aug. 17, 1987, at page 7 (Minn.S.Ct. file #C4-85-1848).

[83] *Videotaped Records of Court Proceedings in the Third, Fifth, and Seventh Judicial Districts*, No. C4-89-2099 (Minn. S. Ct. filed Nov. 17, 1989).

[84] MINN. CODE JUD. COND. § 3A(10); *In Re Modification of Section 3A(10) of the Minnesota Code of Judicial Conduct*, (Minn. S. Ct. filed Jan. 11, 1996); *Audio and Video Coverage of Trial Court Proceedings* (Minn. S. Ct. filed April 18, 1983); *Decree amending Supreme Court Case Dispositional Procedures* (Minn. S. Ct. filed Dec. 11, 1998).

Vital Statistics Records

Most courts have transferred responsibility for handling vital statistics records to local, executive branch agencies. It is expected that this statewide transition will be completed by the end of next year. The advisory committee recommends that, at the end of the transition, ACCESS RULE 6 and its related table be deleted and simply reserved for future use. The state court administrator's office should keep the Minnesota Supreme Court aware of the status of the transition.

Contracts With Vendors for Information Technology Services

Independent contractors performing information technology services for the judicial branch have access to records that are not accessible to the public. A proposed new ACCESS RULE 10 (set forth in Exhibit A) reflects the current practice of the courts in utilizing nondisclosure agreements for such contractors.

Appendices and Tables in the Rules

The ACCESS RULES originally included several appendices that identified then-existing statutes, court rules and other legal authority governing access to a particular case, administrative and vital statistics records. These appendices are in constant need of revision to keep up with new laws, rules and decisions. The advisory committee concluded that modifying the appendices via rule amendment is impractical. The state court administrator maintains updated lists of statutes, court rules and other legal authority governing access to case, administrative and vital statistics records. The current set of lists are set forth in Exhibits R, S and T attached to this report. The committee recommends that regular publication of these lists on the Minnesota Supreme Court's web site take the place of the appendices so that current information is more readily available.

Remedies and Liability for Violations

The advisory committee considered what remedies, if any, are available when a court record custodian fails to comply with the ACCESS RULES. Although court employees can be disciplined for such violations, disciplinary action may not compensate for any resulting damages. For example, the committee considered what remedy is available to a business owner whose trade secret information is improperly disclosed by a court administrator contrary to a protective order? What remedy lies for a person who has had criminal charges dismissed and expunged, but who later loses a job opportunity because court staff improperly

disclosed the expunged record? What would be the basis for a damages claim in such situations, and what, if any, immunity would apply?

The possibility of official liability exposure against the government entity (as opposed to an individual court employee) exists under the state tort claims act, which authorizes claims for "injury to or loss of property or personal injury or death caused by an act or omission of an employee of the state while acting within the scope of office or employment."[85] Statutory exceptions to this liability, also referred to as statutory immunity, exist where an employee is exercising due care in the execution of a valid or invalid statute or rule, or is performing a discretionary duty, whether the discretion is abused.[86] Although judges certainly have authority to exercise discretion in making decisions about access to records, court administrators typically do not. Thus, in the absence of due care, a claim for damages under the state tort claims act for a court administrator's improper disclosure of records would likely not be shielded by statutory immunity.

Similarly, the common-law doctrine of official immunity insulates discretionary action of a public employee at the operational level (as opposed to the planning level), but the discretion exercised must be more than a ministerial act.[87] To be ministerial, the duty must be absolute, certain and imperative, involving merely the execution of a specific duty arising from fixed and designated facts.[88] As discussed above, judges have discretionary authority in regard to record access issues, but court administrators typically do not. Thus, a claim for damages under the state tort claims act for a court administrator's improper disclosure of records would likely not be shielded by common-law official immunity.[89]

---

[85] MINN. STAT. § 3.736, subd. 1 (2002). The total liability is $300,000 for a single claimant and $1,000,000 for any number of claims arising out of a single occurrence. MINN. STAT. § 3.736, subd. 4 (2002).

[86] MINN. STAT. § 3.736, subd. 3 (a), (b) (2002).

[87] *S.W. v. Spring Lake Park School Dist. No. 16*, 580 N.W.2d 19 (Minn. 1998).

[88] *Id*.

[89] Even if the individual employees are held immune, there is no automatic extension of such immunity to the employer. *S.W. v. Spring Lake Park School Dist. No. 16*, 592 N.W.2d 870 (Minn. App. 1999) (refusing to extend vicarious immunity to employer where employees were held immune on basis that extending immunity would reward public body for failure to develop and implement a basic security policy); *affirmed without opinion*, 606 N.W.2d 61 (Minn. 2000).

The possibility of individual liability exposure exists under the federal deprivation of rights statute.[90] Although the state and its employees cannot be sued in their official capacity under this federal statute,[91] state officials may be sued in their individual capacity under this federal statute,[92] subject to available common-law immunities.[93] The United States Supreme Court has granted absolute immunity from personal liability to a very limited class of officials whose special functions or constitutional status requires complete protection from suit, including the President, legislators carrying out their legislative functions, and judges carrying out their judicial (i.e., adjudicatory) functions.[94] These same officials receive at best only a reduced or qualified immunity from personal liability for administrative employment decisions.[95] Lower courts have issued conflicting decisions on whether court administrative staff is clothed with this same immunity when performing a duty that is part of a judicial process.[96] Given the ministerial

---

[90] 42 U.S.C. § 1983 (2003).

[91] *Will v. Mich. Dept. of State Police*, 491 U.S. 58, 109 S.Ct. 2304, 105 L.Ed.2d 45 (1989) (suits against state officials acting in their official capacity are suits against the state, and the state is not a "person" who is subject to § 1983).

[92] 42 U.S.C. § 1983 states:

> Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress, except that in any action brought against a judicial officer for an act or omission taken in such officer's judicial capacity, injunctive relief shall not be granted unless a declaratory decree was violated or declaratory relief was unavailable. For the purposes of this section, any Act of Congress applicable exclusively to the District of Columbia shall be considered to be a statute of the District of Columbia.

[93] *Hafer v. Maleo*, 502 U.S. 21, 112 S.Ct. 358, 116 L.Ed.2d 301 (1991).

[94] *Id.*

[95] *Id.*, citing *Forrester v. White*, 484 U.S. 219, 108 S.Ct. 538, 98 L.Ed.2d 555 (1988) (dismissal of court employee by judge).

[96] *Compare Morrison v. Jones*, 607 F.2d 1269, 1273 (9th Cir. 1979) (immunity from claim that plaintiff failed to receive notice of an order) *with McCray v. State of Maryland*, 456 F.2d 1 (4th Cir. 1972) (no immunity where alleged negligence of clerk in failing to file document had impeded postconviction review).

nature of the duty of court administrative staff to protect certain records from public disclosure, it is unlikely that the federal courts would extend immunity to a wrongful disclosure situation.[97]

Liability may also arise under the invasion of privacy tort recently recognized by the Minnesota Supreme Court.[98] The tort of invasion of privacy recognized in Minnesota takes on three forms: (1) intrusion upon seclusion; (2) publication of private facts; and (3) appropriation. Publication of private facts is the most likely form of the tort to be used for an improper disclosure claim.

Publication of private facts requires: (1) public disclosure; (2) of a private fact; (3) which would be offensive and objectionable to a reasonable person; (4) which is not of legitimate public concern; and (5) which proximately caused damages to plaintiff.[99] Although newsworthiness precludes the recovery of damages, this preclusion may apply only when the facts at issue were contained in a record that is accessible to the public.[100] The tort may not be recognized when the private facts are communicated only to a single person or small group of people.[101] Thus, if the recipients of wrongfully disclosed court records do not further disclose the records, there may be no liability. If the recipients redisclose or publish the records, the claim would appear to be viable.

The advisory committee is also aware of the liability for executive branch agencies for violations of the Data Practices Act; such liability includes: (1) civil action against the governmental unit for damages, including costs and attorney fees, plus exemplary damages of up to $10,000 if the violation is willful; (2) injunctive relief; and (3) action to compel compliance including attorney fees and a civil penalty of up to $300 if the court compels compliance.[102] Willful violations also

---

[97] *Id.*

[98] *Lake v. Wal-Mart*, 582 N.W.2d 231 (Minn. 1998).

[99] *Id.*, citing Restatement (Second) of Torts § 652D (1977).

[100] *See, e.g., Cox Broadcasting v. Cohn*, 420 U.S. 469, 95 S.Ct. 1029, 43 L.Ed.2d 328 (1975).

[101] *Bodah v. Lakeville Motor Express*, 663 N.W.2d 550 (Minn. 2003) (privacy tort for publication of private facts; insufficient publication where social security numbers were distributed to 16 terminal managers); *Robbinsdale Clinic, P.A. v. Pro-Life Action Ministries*, 515 N.W.2d 88, 92 (Minn. App. 1994).

[102] MINN. STAT. § 13.08 (2002) (in determining whether to impose the $300 civil penalty, the court must consider whether the entity has substantially complied with requirements such as designating a responsible authority to receive access requests, designating a compliance official, preparing public documents that identify the responsible authority and the classification of records held by the

(footnote continued next page)

create personal exposure for individuals in the form of misdemeanor criminal charges and just cause for suspension or dismissal from employment.[103]

The advisory committee vigorously discussed five options to address liability: (1) insert in the ACCESS RULES the same penalty provisions that are provided in the Data Practices Act.; (2) retain the status quo and simply rely on existing law without any reference to the issue in the ACCESS RULES; (3) retain status quo and state, without providing or imposing immunity, that the ACCESS RULES do not create any new cause of action; (4) insert a clause in the ACCESS RULES indicating that, absent willful or malicious violations, the ACCESS RULES do not create any new cause of action; (5) insert a clause in the ACCESS RULES indicating that, absent willful or malicious violations, there shall be no liability for violations of the ACCESS RULES.

Some advisory committee members believe that it is not fair to impose the executive branch Data Practices Act liability on a court because the scope of the court's role is so much broader than the typical executive branch entity, a court cannot reasonably control every piece of information that makes its way into the court's files, and the fear of such liability will stifle public access and result in denials of hundreds of daily access requests that are now routinely granted. For example, if a judge fails to keep all social security numbers or victim identifying information out of a judgment or order and then files it with the court administrator, who then provides public access to the judgment or order, it is the court administrator who will be sued for the violation, not the judge. The next time a request for similar documents arises, the court administrator will seek legal counsel who will advise the administrator to disclose it only if the recipient agrees to indemnify the administrator or the court issues an order authorizing the disclosure. The time and cost associated with obtaining such an agreement or order has the potential to bring effective public access to a halt. Such problems are not present if liability is limited to willful or malicious disclosures only.

Other advisory committee members favor liability for inadvertent disclosures, citing recent case law (invasion of privacy tort discussed above) that allows a damages claim for disclosure of social security numbers by a private entity, and the absence of a complete shutdown of access under the current exposure to liability. These members also question whether the court can in essence trump the state tort claims statute by declaring that there can be no liability for anything

---

(footnote continued from previous page)
entity, developing access procedures, requesting and following advisory opinions from the department of administration, and training entity personnel).

[103] MINN. STAT. § 13.09 (2002).

other than willful or malicious violations of the ACCESS RULES. Other members explain that establishing the limits of liability is a part of establishing the duty to protect certain court records. The court has established immunity by court rule in other contexts that include record access duties.[104]

A majority of the committee determined that the ACCESS RULES should expressly state that, absent willful or malicious violations, there shall be immunity from liability for violations of the ACCESS RULES. This position is set forth in proposed ACCESS RULE 11 (see Exhibit A to this report).

Expungement

Expungement is a process where a party can request that a case, record or conviction be made to effectively 'disappear' from the court's records either completely or partially. Two types of criminal court record[105] expungement are available in Minnesota. One is a statutory procedure that is available only in limited circumstances[106] and results in sealing of the record and prohibiting its

[104] *See, e.g.,* MINN. R. BD. JUD. STDS. 3 (members of the Board on Judicial Standards are absolutely immune from suit for all conduct in the course of their official duties); MINN. R. LAWYERS PROF. RESP. 21(b) (Lawyers Professional Responsibility Board members, other panel members, District Committee members, the Director, and the Director's staff, and those entering agreements with the Director's office to supervise probation are immune from suit for any conduct in the course of their official duties); MINN. R. ADMISSION TO THE BAR 12.A. (The Board of Law Examiners and its members, employees and agents are immune from civil liability for conduct and communications relating to their duties under the Rules of Admission to the Bar or the Board's policies and procedures); MINN. R. BD. LEGAL CERT. 120 (the Board of Legal Certification and its members, employees, and agents are immune from civil liability for any acts conducted in the course of their official duties); MINN. R. CLIENT SEC. BD. 1.05 (the Client Security Board and its staff are absolutely immune from civil liability for all acts in the course of their official capacity).

[105] If there is no criminal complaint, indictment, traffic ticket or tab charge filed in court (e.g., the prosecutor diverted the case or determined not to file charges), and the individual has a clean record for the past 10 years, a petition to the court is not necessary to expunge an arrest record. There is a statutory procedure that the individual can invoke directly through the executive branch department(s) that maintain arrest records such as the arresting agency and/or the Minnesota Bureau of Criminal Apprehension. MINN. STAT. § 299C.11(b) (2003).

[106] To qualify for expungment, an individual must have: (1) been charged with possession of a controlled substance under sections 152.18, subd. 1, 152.024, 152.052, or 152.027 and the proceedings were dismissed and discharged; or (2)

(footnote continued next page)

disclosure except under certain conditions;[107] this procedure also applies to criminal records held by certain executive branch agencies such as law enforcement and the Bureau of Criminal Apprehension.[108] The other is derived from the constitution and affects only court records; it generally would not reach any records held by state or local executive branch agencies such as law enforcement or the BCA.[109]

Forms and instructions for requesting statutory expungement are available from the state court website,[110] and overall these documents provide clear direction to litigants. The advisory committee believes, however, that litigants should also be educated about the limitations of expungements such as the fact that expungement of a court record does not automatically require a private sector enterprise to delete the information from its records,[111] or that statutory expungement will not

---

(footnote continued from previous page)
been a juvenile prosecuted as an adult and finally discharged by the commissioner of corrections or placed on probation and then discharged from probation; or (3) all pending actions or proceedings resolved in the individual's favor (e.g., charges were dismissed, found not guilty, or case did not otherwise result in a conviction. MINN. STAT. § 609A.02, subds. 1 - 4. (2003) (records of conviction for an offense for which registration is required under section 243.166 may not be expunged).

[107] Law enforcement agencies, prosecution or correctional authorities may seek an order to re-open a sealed record for the purpose of a criminal investigation, prosecution or sentencing, and the record may be opened without a court order for the purposes of evaluating a prospective employee of a criminal justice agency. MINN. STAT. § 609A.03, subd. 7 (2003).

[108] MINN. STAT. § 609A.01 (2003). DNA samples and DNA records held by the Bureau of Criminal Apprehension, that are related to a charge supported by probable cause, are not subject to sealing under the expungement statute. MINN. STAT. § 609A.03, subd. 7 (2003).

[109] *State v. C.A.*, 304 N.W.2d 353 (Minn. 1981) (inherent authority of the court to seal its own records where necessary to prevent serious infringement of constitutional rights); *State v. Ambaye*, 616 N.W.2d 256 (Minn. 2000) (same); see State v. T.M.B., 590 N.W.2d 809 (Minn. Ct. App. 1999) (court lacks inherent authority to seal records maintained by executive branch unless there is a showing that the executive agents abused their discretion in the performance of a governmental function).

[110] At www.courts.state.mn.us, click on "Clerks Office" then click on "Court Forms," then select "Criminal," then scroll down to "Expungement."

[111] Some private enterprises may be required by laws such as the Fair Credit Reporting Act to refrain from reporting certain information that is no longer verifiable through court records, but a litigant may have to take steps in addition to
(footnote continued next page)

remove a firearms restriction imposed for a crime of violence.[112] Litigants should be aware of such limitations before beginning the expungement process, which can be both complex and costly.[113]

Effective Date

The advisory committee believes that while these recommendations may require a few months lead time to allow the courts and litigants to prepare for their implementation, it should be feasible to adopt them in late 2004 and have them take effect on January 1, 2005. The remote access provisions have built into them a practicality standard that requires Internet posting to the extent that the court has the technical capacity and resources to do so. The Minnesota Supreme Court has established a Technology Planning Committee that oversees the state funded technical resources and capacity for the court system. Through the TPC, for example, the transition of the trial courts to their new, statewide case management computer system (MNCIS) will involve a conversion of the majority of pending cases from the previous systems (minus those no longer retained through longstanding record retention schedules). As the remainder of the districts become state funded, this review will centralize, although some local ability may remain to post calendars and similar items that are currently found on some of the individual judicial district websites. Thus, it is anticipated that Internet access to court generated documents such as judgments and orders will be addressed on a statewide, or project-wide, basis, with due consideration given to technical capacity and resources.

(footnote continued from previous page)
obtaining the expungement to make this happen. *See, e.g.*, 15 U.S.C. § 1681i(a)(5) (2004) (if aconsumer disputes information in his credit file by filing a dispute with the consumer reporting agency, and the consumer reporting agency can no longer verify the information, it must be removed from the credit report).

[112] MINN. STAT. § 609A.03, subd. 5a (Supp. 2003).

[113] The procedure requires a detailed petition, service on the prosecutor and all entities whose records would be subject to the order, a hearing at which the judge determines whether the benefits of expungement outweigh the disadvantages to the public and public safety, an automatic stay of any order for 60 days plus the time period of an appeal, and a filing fee of $235 (no fees required if pauper status is granted or all pending proceedings were resolved in favor of the individual). MINN. STAT. §§ 609A.03; (2003).

Follow Up

The advisory committee's go-slow recommendation for Internet access to court records contemplates a follow up review. The committee believes that a one-time review should be conducted within six to twelve months after Internet access to court records has been implemented, and that continuity in committee membership is important to the thoroughness and efficiency of such a review process. The advisory committee recommends that an order reinstituting the committee should be made at the appropriate time.

EXHIBITS

Exhibit A: Proposed Changes To The Rules Of Public Access To Records Of The Judicial Branch

Key: Additions to the rules are indicted by underlined text and deletions indicated by strikeout text.

Rule 1. Scope of Rules.

These rules govern access to the records of all courts and court administrators of the judicial branch of the state of Minnesota. They do not govern access to records of the Tax Court or the Workers' Compensation Court of Appeals, which are part of the executive branch of the state. In addition, these rules do not govern access to records of the various Boards or Commissions of the Supreme Court as they are governed by independent rules promulgated or approved by the Supreme Court. A partial list of Boards and Commissions is set forth in Appendix A.

Finally, except as provided in Rule 4, subdivision 1(b) with respect to case records, these rules do not govern access to records of court services departments or probation authorities. Access to these records is governed by other applicable court rules and statutes, including ~~Minnesota Statutes, section~~ MINN. STAT. § 13.84 and its successor.

Nothing in these rules shall affect the disposition of records pursuant to ~~Minnesota Statutes, section~~ MINN. STAT. § 138.17 or its successor or prevent the return of documents or physical objects to any person or party pursuant to a court rule or order.

Rule 2. General Policy.

Records of all courts and court administrators in the state of Minnesota are presumed to be open to any member of the public for inspection or copying at all times during the regular office hours of the office having custody of the records. Some records, however, are not accessible to the public, at least in the absence of a court order, and these exceptions to the general policy are set out in Rules 4, 5, ~~and~~ 6, and 8.

Rule 3. Definitions.

Subd. 1. Custodian. The custodian is the person responsible for the safekeeping of any records held by any court or court administrator's or clerk of court's office. In the absence of the person usually responsible, the person who is temporarily responsible for the records is the custodian. For purposes of remote and bulk electronic access under Rule 8, the state court administrator shall be the custodian for case records that are maintained in computer systems administered by the state court administrator's office.

Subd. 2. Judge. "Judge" means any justice, judge, judicial officer, referee, court-appointed arbitrator or other person exercising adjudicatory powers.

Subd. 3. Court. "Court" means the Supreme Court, the Court of Appeals, District, Juvenile, Family, Conciliation, County and Probate Court, and any other court established as part of the judicial branch of the state.

Subd. 4. Court Administrator. "Court administrator" means a person employed or appointed for the purpose of administering the operations of any court or court system, including the offices of judicial district administrator, court administrators of the respective counties, and state-wide court administrative agencies.

Subd. 5. Records. "Records" means any recorded information that is collected, created, received, maintained, or disseminated by a court or court administrator, regardless of physical form or method of storage. A "record" does not necessarily constitute an entire file, as a file may contain several "records." Court reporters' notes shall be available to the court for the preparation of a transcript.

(a) Case Records. "Case records" means all records of a particular case or controversy.

(b) Administrative Records. "Administrative records" means all records pertaining to the administration of the courts or court systems.

(c) Vital Statistics Records. "Vital statistics records" means all certificates or reports of birth, death, fetal death, induced abortion, marriage, dissolution and annulment, and related records.

Rule 4. Accessibility to Case Records.

Subd. 1. Accessibility. All case records are accessible to the public except the following:

(a) *Domestic Abuse Records*. Records maintained by a court administrator pursuant to the domestic abuse act, ~~Minnesota Statutes, section~~ MINN. STAT. § 518B.01, until a ~~temporary~~ court order made pursuant to subdivision 5 or 7 of section 518B.01 is executed or served upon the record subject who is the respondent to the action;

(b) *Court Services Records*. Records on individuals maintained by a court, other than records that have been admitted into evidence, that are gathered at the request of a court:

(1) to determine an individual's need for counseling, rehabilitation, treatment or assistance with personal conflicts,

(2) to assist in assigning an appropriate sentence or other disposition in a case,

(3) to provide the court with a recommendation regarding the custody of minor children, and

(4) to provide the court with a psychological evaluation of an individual.

Provided, however, that the following information on adult individuals is accessible to the public: name, age, sex, occupation, and the fact that an individual is a parolee, probationer, or participant in a diversion program, and if so, at what location; the offense for which the individual was placed under supervision; the dates supervision began and ended and the duration of supervision; information which was public in a court or other agency which originated the data; arrest and detention orders; orders for parole, probation or participation and the extent to which those conditions have been or are being met; identities of agencies, units within agencies and individuals providing supervision; and the legal basis for any change in supervision and the date, time and locations associated with the change.

(c) *Judicial Work Product and Drafts.* All notes, memoranda or drafts thereof prepared by a judge or by a court employed attorney, law clerk, legal assistant or secretary and used in the process of preparing a final decision or order, except the official minutes prepared pursuant to ~~Minnesota Statutes, sections~~ MINN. STAT. §§ 546.24-.25.

(d) ~~*Criminal Cases;*~~ *Juvenile Appeal Cases*. ~~Case records that are made inaccessible to the public pursuant to the rules of criminal procedure or the rules of procedure for the juvenile courts.~~ Case records arising from an appeal from juvenile court proceedings that are not open to the public, except the written opinion resulting from the appeal, are inaccessible to the public unless otherwise provided by rule or order of the appellate court.

(e) *Race Census Records.* The contents of completed race census forms obtained from participants in criminal, traffic, juvenile and other matters, except that the records may be disclosed in bulk format if the recipient of the records:

(1) executes a nondisclosure agreement in a form approved by the state court administrator in which the recipient of the records agrees not to disclose to any third party any information in the records from which the identity of any participant or other characteristic that could uniquely identify any participant is ascertainable; and

(2) the custodian of the records reasonably determines that disclosure to the recipient will not compromise the confidentiality of any participant's race status.

(f) *Other~~Records Controlled by Statute~~*. Case records that are made inaccessible to the public pursuant to:

(1) state statutes, other than Minnesota Statutes, chapter 13;

(2) court rules or orders; or

(3) other applicable law.

~~A~~The state court administrator shall maintain, publish and periodically update a partial list of case records that are not accessible to the public ~~is set forth in Appendix B~~.

~~(f) *Civil Cases.* Case records made inaccessible to the public by protective or other order of the court.~~

Subd. 2. Restricting Access; Procedure. Procedures for restricting access to case records shall be as provided in the applicable court rules ~~of civil and criminal procedure~~.

Advisory Committee Comment~~Note~~ 2004

The 2004 deletion of the word "temporary" in Rule 4, subd. 1(a), reflects statutory changes that allow the initial, ex parte order to be the permanent order of the court if no hearing is requested. See 1995 MINN. LAWS ch. 142, §§ 4, 5 (amending MINN. STAT. § 518B.01, subds. 5, 7).

The 2004 reorganization of Rule 4, subd. 1, parts (d) and (f) is not substantive in nature. Documents admitted into evidence are also addressed in Rule 8, subd. 4. The substitution of a periodically updated list of inaccessible case records for Appendix B in Rule 4, subd. 1(e) recognizes that the state court administrator maintains an updated list of statutes (and court rules and other legal authority) that identify case records that are not accessible to the public. The list is updated as necessary, whereas Appendix B quickly became obsolete soon after it was first published. It is contemplated that the list would be posted on the Court's website for access by the general public.

The 2004 addition of race census records in Rule 4, subd. 1(e) is based on the understanding that race and ethnicity information is not solicited from participants for the purpose of reselling race status of individuals to commercial enterprises. The goal is to ensure fair resolution of cases, and the rule attempts to provide a limited right of public access consistent with that goal. Access to race census records, e.g., for research purposes, can be obtained pursuant to a nondisclosure agreement that limits ultimate public disclosure to aggregate statistics that do not identify individual participants. The court has a longstanding tradition of authorizing disclosure of juvenile court records for scholarly research using nondisclosure agreements. *See, e.g., Order Authorizing*

Disclosure of Juvenile Court Database for Research Purposes, No. C4-85-1848 (Minn. S. Ct. filed May 14, 2001). The custodian's duty to make a reasonable determination that disclosure will not compromise the identity of individuals is taken from the "summary data" provisions of the executive branch Data Practices Act. MINN. STAT. §§ 13.02, subd. 19; 13.05, subd.7, (2003).

The 2004 changes to Rule 4, subd. 2, recognize that a variety of rules address restrictive orders. The factors to consider in seeking a protective order in regard to criminal case records are discussed in Rule 25, Rules of Criminal Procedure, *Minneapolis Star & Tribune v. Kammeyer*, 341 N.W.2d 550 (Minn. 1983), and *Northwest Publications, Inc. v. Anderson*, 259 N.W.2d 254 (Minn. 1977). For civil cases, see Rule 26.03, Rules of Civil Procedure and *Minneapolis Star & Tribune v. Schumacher*, 392 N.W.2d 197 (Minn. 1986). For child in need of protective services cases, see Rule 44.07, Rules of Juvenile Procedure. For juvenile delinquency cases, see Rule 10.05, subd. 5, Rules of Juvenile Procedure.

Rule 5. Accessibility to Administrative Records.

All administrative records are accessible to the public except the following:

Subd. 1. ~~Employee~~Personnel Records. Records on individuals collected because the individual is or was an employee of, performs services on a voluntary basis for, or acts as an independent contractor with the judicial branch, provided, however, that the following information is accessible to the public: name; actual gross salary; salary range; contract fees; actual gross pension; the value and nature of employer-paid fringe benefits; the basis for and the amount of any added remuneration, including expense reimbursement, in addition to salary; job title and bargaining unit; job description; education and training background; previous work experience; date of first and last employment; the status of any complaints or charges against the employee, whether or not the complaint or charge resulted in a disciplinary action; the final disposition of any disciplinary action and supporting documentation, excluding information that would identify confidential sources who are employees of the judicial branch; the terms of any agreement settling any dispute arising out of an employment relationship; work location; a work telephone number; honors and awards received; payroll time sheets or other comparable data, that are only used to account for employee's work time for payroll purposes, to the extent that they do not reveal the employee's reasons for the use of sick or other medical leave or other information that is not public; and ~~city and~~ county of residence~~;~~.

(a) For purposes of this subdivision, a final disposition occurs when the person or group that is authorized to take the disciplinary action makes its final decision about the disciplinary action, regardless of the possibility of any later court proceedings or other proceedings. In the case of arbitration proceedings arising under collective bargaining agreements, a final disposition occurs at the conclusion of the arbitration proceedings, or upon the failure of the employee to elect arbitration within the time provided by the collective bargaining agreement. Final disposition includes a resignation by an individual when the resignation

occurs after the final decision of the person or group that is authorized to take disciplinary action, or arbitrator.

(b) Notwithstanding contrary provisions in these rules, a photograph of a current or former employee may be displayed to a prospective witness as part of an investigation of any complaint or charge against the employee.

(c) Notwithstanding contrary provisions in these rules, if an appointed officer resigns or is terminated from employment while the complaint or charge is pending, all information relating to the complaint or charge is public, unless access to the information would jeopardize an active investigation or reveal confidential sources. For purposes of this paragraph, "appointed officer" means the clerk of the appellate courts, the state court administrator, a judicial district administrator, and a court administrator of district court.

(d) Records under subdivision 1 may be disseminated to a law enforcement agency for the purpose of reporting a crime or alleged crime committed by an employee, volunteer or independent contractor, or for the purpose of assisting law enforcement in the investigation of a crime committed or allegedly committed by an employee, volunteer, or independent contractor.

(e) Records under subdivision 1 must be disclosed to the department of employment and economic development for the purpose of administration of an unemployment benefits program under state law.

(f) Records under subdivision 1 may be disseminated to labor organizations to the extent that the custodian determines that the dissemination is necessary to conduct elections, notify employees of fair share fee assessments, and implement the provisions of Minnesota Statutes, section 179 and 179A. Records under subdivision 1 shall be disseminated to labor organizations and to the bureau of mediation services to the extent the dissemination is ordered or authorized by the Commissioner of the Bureau of Mediation Services.

(g) If the custodian determines that the release of records under subdivision 1 is necessary to protect an employee, volunteer or independent contractor from harm to self or to protect another person who may be harmed by the employee, volunteer, or independent contractor, records that are relevant to the concerns for safety may be released to: the person who may be harmed and to the person's attorney when the records are relevant to obtaining a restraining order; to a prepetition screening team conducting an investigation under section 253B.07, subdivision 1; or to a court, law enforcement agency, or prosecuting authority. If the person who may be harmed or the person's attorney receives records under this subdivision, the records may be used or released further only to the extent necessary to protect the person from harm.

Subd. 2. Applicant Records. Records on individuals collected because the individual is or was an applicant for employment with the judicial branch, provided, however, that the following information is accessible to the public: veteran status; relevant test scores; rank on eligible lists; job history; education and training; work availability; and, after the applicant has been certified by the appointing authority to be a finalist for a position in public employment, the name of the applicant~~;~~.

Subd. 3. Correspondence. Correspondence between individuals and judges; but such correspondence may be made accessible to the public by the sender or the recipient.

Subd. 4. Schedules and Assignments. The identity of appellate judges or justices assigned to or participating in the preparation of a written decision or opinion, until the decision or opinion is released~~;~~.

Subd. 5. Security Records. Records that would be likely to substantially jeopardize the security of information, possessions, individuals, or property in the possession or custody of the courts against theft, tampering, improper use, illegal disclosure, trespass, or physical injury such as security plans or codes~~;~~.

Subd. 6. State Owned or Licensed Trade Secrets. Records revealing a common law trade secret or a trade secret as defined in M.S.A. 325C.01 that is the property of the state and is maintained by a court or court administrator; provided, that the following are accessible to the public: the existence of any contract, the parties to the contract, and the material terms of the contract, including price, projected term, and scope of work.~~;~~

Subd. 7. Copyrighted Material. Computer programs and related records, including but not limited to technical and user manuals, for which the judicial branch has acquired or is in the process of acquiring, including through licensing in whole or in part, a patent or copyright; provided, that the following are accessible to the public: the existence of any contract, the parties to the contract, and the material terms of the contract, including price, projected term, and scope of work.~~;~~

Subd. 8. Competitive Bidding Records.

(a) Sealed Bids. Sealed bids and responses to judicial branch bid or procurement requests or solicitations, including the number of bids or responses received, shall be inaccessible to the public prior to the opening of the bids or responses at the time specified in the judicial branch ~~bid~~ request or solicitation.

(b) Submission of Trade Secret. Except as provided in subparagraph (c) of this rule, a common law trade secret or a trade secret as defined in ~~Minn. Stat.~~ MINN. STAT. § 325C.01~~,~~ that is required to be submitted pursuant to a judicial branch bid or procurement request~~,~~ shall be inaccessible to the public provided that:

(1) the ~~bidder~~ submitting party marks the document(s) containing the trade secret "CONFIDENTIAL;"

(2) the ~~bidder~~ submitting party submits as part of the bid or response a written request to maintain confidentiality; and

(3) the trade secret information is not publicly available, already in the possession of the judicial branch, or known to or ascertainable by the judicial branch from third parties.

(c) Contract. The following are accessible to the public: the existence of any resulting contract, the parties to the contract, and the material terms of the contract, including price, projected term, and scope of work.

Subd. 9. Compliance Records. Records and reports and drafts thereof maintained by the State Judicial Information Systems and the Trial Court Information Systems for purposes of compliance with ~~Minnesota Statutes, section~~ MINN. STAT. § 546.27~~;~~.

Subd. 10. Library Records. Records maintained by the state law library which: (a) link a patron's name with materials requested or borrowed by the patron or which links a patron's name with a specific subject about which the patron has requested information or materials; or (b) are submitted by a person applying for a borrower's card, other than the name of the person to whom a borrower's card has been issued.~~;~~

Subd. 11. Passport Records. Passport applications and accompanying documents received by court administrators, and lists of applications that have been transmitted to the United States Passport Office~~;~~.

Subd. 12. Attorney Work Product. The work product of any attorney or law clerk employed by or representing the judicial branch that is produced in the regular course of business or representation of the judicial branch.

Subd. 13. Other. Matters that are made inaccessible to the public pursuant to:

(a) state statute, other than Minnesota Statutes, chapter 13, or
(b) federal law; or
(c) rule or order of the Supreme Court.

~~A~~The state court administrator shall maintain, publish and periodically update a partial list of administrative records that are not accessible to the public ~~is set forth in Appendix C~~.

Advisory Committee Comment-2004

The 2004 changes to Rule 5, subd. 1, are based on policy applicable to employee records held by the executive branch. MINN. STAT. § 13.43 (2002). There are some subtle differences from executive branch policy, however, including the fact that judicial discipline is governed by a separate set of procedures and access provisions. RULES OF THE BOARD ON JUDICIAL STANDARDS. In addition, judicial branch email addresses are not accessible to the public unless individual employees authorize disclosure. This helps minimize potential for ex parte contact prohibited by law. CODE JUD. CONDUCT § 3.A(7).

The 2004 changes to Rule 5, subds. 6, 7 and 8, reflect the existing practice. Trade secrets and copyrights are subject to state and federal law, and the specifics are generally clarified in procurement documents, from requests for bids to contracts, in the manner set forth in the rule. Once a vendor enters into a contract, the basic parameters of the contract relationship become accessible under Rule 5, subd. 1. These revisions provide notice to potential vendors of what to expect and ensure consistent results.

The 2004 changes to Rule 5, subd. 10, regarding library records provides consistent protection to information held by the library.

The 2004 substitution of a periodically updated list for Appendix C in Rule 5, subd. 13 recognizes that the state court administrator maintains an updated list of statutes (and court rules and other legal authority) that identify administrative records that are not accessible to the public. The list is updated as necessary, whereas Appendix C became obsolete soon after it was first published. It is contemplated that the list would be posted on the Court's website for access by the general public.

Rule 6. Vital Statistics Records.

Vital statistics records held by any court or court administrator shall be accessible to the public except as provided by statute. ~~A~~The state court administrator shall maintain, publish and periodically update a partial list of vital statistics records that are not accessible to the public ~~is set forth in Appendix D~~.

Advisory Committee Comment –2004

The 2004 substitution of a periodically updated list for Appendix D in Rule 6 recognizes that the state court administrator maintains an updated list of statutes (and court rules and other legal authority) that identify vital statistics records that are not accessible to the public. The list is updated as necessary, whereas Appendix D became obsolete soon after it was first published. It is contemplated that the list would be posted on the Court's website for access by the general public.

Rule 7. Procedure for Requesting Access or Correction.

Subd. 1. To Whom Request is Made. A request to inspect or obtain copies of records that are accessible to the public shall be made to the custodian and may be made orally or in writing. The custodian may insist on a written request only if the complexity of the request or the volume of records requested would jeopardize the efficiency and accuracy of the response to an oral request. All requests must include sufficient information to reasonably identify the data being sought, but the requesting person shall not be required to have detailed knowledge of the agency's filing system or procedures, nor shall the requesting person be required to disclose the purpose of the request.

Subd. 2. Response. The custodian shall respond to the request as promptly as practical.

Subd. 3. Delay or Denial; Explanation. If a request cannot be granted promptly, or at all, an explanation shall be given to the requesting person as soon as possible. The requesting person has the right to at least the following information: the nature of any problem preventing access, and the specific statute, federal law, or court or administrative rule that is the basis of the denial. The explanation shall be in writing if desired by the requesting person. Appeals are governed by Rule 9 of these rules.

Subd. 4. Referral in Certain Cases. If the custodian is uncertain of the status of the record, the custodian may ask for a determination from the office of the state court administrator. The state court administrator shall promptly make a determination and forward it either orally or in writing~~by phone or by mail~~ to the custodian.

Subd. 5. Correction of Case Records. An individual who believes that a case record contains clerical errors may submit a written request for correction, no longer than two pages, to the court administrator of the court that maintains the record, with a copy served on all parties to the case. The court administrator shall promptly do one of the following: (a) correct a clerical error for which no court order is required; (b) forward the request to the court to be considered informally; or (c) forward the request to the party or participant who submitted the record containing the alleged clerical error who in turn may seek appropriate relief from the court. Upon forwarding under clause (b), the court may either correct the error on its own initiative or direct that the request will only be considered pursuant to a motion requesting correction. The court's directive may also establish appropriate notice requirements for a motion. This procedure need not be exhausted before other relief is requested.

Advisory Committee Comment-2004

The 2004 addition in Rule 7, subd. 3, of a cross reference to appeals under Rule 9 is added as a convenience to counterbalance the growing complexity of these rules. The 2004 deletion of the term "mail" in Rule 7, subd. 4, recognizes that a determination is often issued in electronic format, such as email or facsimile transmission.

The 2004 addition of subdivision 5 regarding correction of records is based in part on MINN. GEN. R. PRAC. 115.11 (motion to reconsider). In the context of Internet publication of court records, a streamlined process is particularly appropriate for clerical-type errors, and should allow for prompt resolution of oversights and omissions. For example, to the extent that the register of actions, court calendar, or index in a court's case management system incorrectly incorporates provisions of a court order, judgment, or pleading, such data entry inaccuracies are typically corrected without a court order by court administration staff promptly upon learning of the inaccuracy.

A party is not required to utilize the procedure set forth in subdivision 5 before making a formal motion for correction of a case record in the first instance. Alleged inaccuracies in orders and judgments themselves must be brought to the attention of the court in accordance with procedures established for that purpose. Clerical errors in judgments and orders typically can be addressed by motion. *See, e.g.*, MINN. GEN. R. PRAC. 375 (expedited child support process; clerical mistakes, typographical errors, and errors in mathematical calculations in orders …arising from oversight or omission may be corrected by the child support magistrate at any time upon the magistrate's own initiative or upon motion of a party after notice to all parties); MINN. R. CIV. P. 60.01 (civil cases; clerical mistakes in judgments, orders, or other parts of the record and errors therein arising from oversight or omission may be corrected by the court at any time on its own initiative or on the motion of any party after such notice, if any, the court orders); MINN. R. CRIM. P. 27.03, subds. 8, 9 (criminal cases: clerical mistakes in judgments, orders, or other parts of the record or errors in the record arising from oversight or omission may be corrected by the court at any time and after such notice, if any, as the court orders; the court may at any time correct a sentence not authorized by law); MINN. R. JUV. PROT. P. 41.01 (juvenile protection cases; clerical mistakes in judgments, orders, or other parts of the record and errors arising from oversight or omission may be corrected by the court at any time upon its own initiative or upon motion of any party and after such notice, if any, as the court orders; during the pendency of an appeal, such mistakes can be corrected with leave of the appellate court); MINN. R. CIV. APP. P. 11.05 (differences as to whether the transcript or other parts of the record on appeal truly disclose what occurred in the trial court are to be submitted to and determined by the trial court; material omissions or misstatements may be resolved by the trial court, stipulation of the parties, or on motion to the appellate court).

Alleged inaccuracies in the records submitted by the parties and other participants in the litigation must also be brought to the attention of the court through existing procedures for introducing and challenging evidence. These procedures typically have deadlines associated with the progress of the case and failure to act in a timely fashion may preclude relief.

Rule 8. Inspection, ~~and Photoc~~Copying, Bulk Distribution and Remote Access.

Subd. 1. Access to Original Records. Upon request to a custodian, a person shall be allowed to inspect or to obtain copies of original versions of records that are accessible to the public in the place where such records are normally kept, during regular working hours. However, if access to the original records would result in disclosure of information to which access is not permitted, provide remote or bulk access that is not permitted under this Rule 8, jeopardize the security of the records, or prove otherwise impractical, copies, edited copies, reasonable facsimiles or other appropriate formats may be produced for inspection. Unless expressly allowed by the custodian, records shall not be removed fom the area where they are normally kept.

Subd. 2. Remote Access to Electronic Records.

(a) **Remotely Accessible Electronic Records.** Except as otherwise provided in Rule 4 and parts (b) and (c) of this subdivision 2, a court administrative office that maintains the following electronic case records must provide remote electronic access to those records to the extent that the office has the resources and technical capacity to do so.

(1) **register of actions** (a register or list of the title, origination, activities, proceedings and filings in each case [MINN. STAT. § 485.07(1)]);
(2) **calendars** (lists or searchable compilations of the cases to be heard or tried at a particular court house or court division [MINN. STAT. § 485.11]);
(3) **indexes** (alphabetical lists or searchable compilations for plaintiffs and for defendants for all cases including the names of the parties, date commenced, case file number, and such other data as the court directs [MINN. STAT. § 485.08]);
(4) **judgment docket** (alphabetical list or searchable compilation including name of each judgment debtor, amount of the judgment, and precise time of its entry [MINN. STAT. § 485.073)]);
(5) **judgments, orders, appellate opinions, and notices prepared by the court**.

All other electronic case records that are accessible to the public under Rule 4 shall not be made remotely accessible but shall be made accessible in either electronic or in paper form at the courthouse.

(b) **Certain Data Elements Not To Be Disclosed.** Notwithstanding Rule 8, subd. 2 (a), the public shall not have remote access to the following data elements in an electronic case record with regard to parties or their family members, jurors, witnesses, or victims of a criminal or delinquent act:

(1) social security numbers [and employer identification numbers];
(2) street addresses;
(3) telephone numbers;
(4) financial account numbers; and
(5) in the case of a juror, witness, or victim of a criminal or delinquent act, information that specifically identifies the individual or from which the identity of the individual could be ascertained.

(c) **Preconviction Criminal Records.** Preconviction criminal records shall be made remotely accessible only by using technology which, to the extent feasible, ensures that records are not searchable by defendant name using automated tools. A "preconviction criminal record" is a record for which

there is no "conviction" as defined in Minnesota Statutes, section 609.02, subd. 5 (2003).

(d) **"Remotely Accessible" Defined.** "Remotely accessible" means that information in a court record can be electronically searched, inspected, or copied without the need to physically visit a court facility.

(e) **Exception.** After notice to the parties and an opportunity to be heard, the presiding judge may by order direct the court administrator to provide remote electronic access to records of a particular case that would not otherwise be remotely accessible under parts (a), (b) or (c) of this rule.

[Bulk Data Alternative 1: **Subd. 3. Bulk Distribution of Electronic Case Records.** A court administrative office shall provide bulk distribution of only its electronic case records that are remotely accessible to the public pursuant to subdivision 2 of this rule, to the extent that office has the resources and technical capacity to do so. "Bulk distribution" means distribution of all, or a significant subset, of the court's electronic case records.]

[Bulk Data Alternative 2: **Subd. 3. Bulk Distribution of Electronic Case Records.** "Bulk distribution" means distribution of all, or a significant subset, of the court's electronic case records.

(a) Bulk distribution of information in the court record is permitted for court records that are publicly accessible under Rules 4 and 5.

(b) A request for bulk distribution of information not publicly accessible can be made to the court for scholarly, journalistic, political, governmental, research, evaluation or statistical purposes where the identification of specific individuals is ancillary to the purpose of the inquiry. Prior to the release of information pursuant to this subsection the requestor must comply with the provisions of Rule 8, subd. 3(c).

(c) Bulk distribution that includes information to which public access has been restricted may be requested by any member of the public only for scholarly, journalistic, political, governmental, research, evaluation, or statistical purposes.

(1) The request shall: identify what information is sought, describe the purpose for requesting the information and explain how the information will benefit the public interest or public education, and explain provisions for the secure protection of any information requested to which public access is restricted or prohibited.

(2) The court may grant the request if it determines that doing so meets criteria established by the court and is consistent with the purposes of the access policy, the resources are available to

compile the information, and that it is an appropriate use of public resources.]

[Bulk Data Alternative 3: **Subd. 3. Bulk Distribution of Court Records.** A court administrative office shall, to the extent that office has the resources and technical capacity to do so provide bulk distribution of its electronic case records as follows:

(a) Preconviction criminal records shall be provided only to an individual or entity which enters into an agreement in the form approved by the state court administrator providing that the individual or entity will not disclose or disseminate the data in a manner that identifies specific individuals who are the subject of such data. If the state court administrator determines that a bulk data recipient has utilized data in a manner inconsistent with such agreement, the state court administrator shall not allow further release of bulk data to that individual or entity except upon order of a court.

(b) All other electronic case records that are remotely accessible to the public under Rule 8, Subd. 3 shall be provided to any individual or entity.]

Subd. 4. Criminal Justice and Other Agencies. Criminal justice agencies, including public defense agencies, and other state or local government agencies may obtain remote and bulk case record access where access to the records in any format by such agency is authorized by law.

Subd. ~~2~~5. Access to Certain Evidence. Except where access is restricted by court order or the evidence is no longer retained by the court pursuant to court rule, order or retention schedule, documents and p~~P~~hysical objects admitted into evidence in a proceeding that is open to the public shall be available for public inspection under such condition~~s~~ as the court administrator may deem appropriate to protect the security of the evidence.

Subd. ~~3~~6. Fees. When copies are requested, the custodian may charge the copy fee established pursuant to statute but, unless permitted by statute, the custodian shall not require a person to pay a fee to inspect a record. When a request involves any person's receipt of copies of publicly accessible information that has commercial value and is an entire formula, pattern, compilation, program, device, method, technique, process, data base, or system developed with a significant expenditure of public funds by the judicial branch, the custodian may charge a reasonable fee for the information in addition to costs of making, certifying, and compiling the copies. The custodian may grant a person's request to permit the person to make copies, and may specify the condition under which this copying will be permitted.

Advisory Committee Comment-2004

The 2004 addition of a new Rule 8, subd. 2, on remote access establishes a distinction between public access at a courthouse and remote access over the Internet. Subdivision 2 attempts to take a measured step into Internet access that provides the best chance of successful

implementation given current technology and competing interests at stake. The rule limits Internet access to records that are created by the courts themselves as this is the only practical method of ensuring that necessary redaction will occur. Redaction is necessary to prevent Internet access to clear identity theft risks such as social security numbers and financial account numbers. The rule recognizes a privacy concern with respect to remote access to telephone and street addresses, or the identities of witnesses or jurors or crime victims. The identity of victims of a criminal or delinquent act are already accorded confidentiality in certain contexts [MINN. STAT. § 609.3471 (2002) (victims of criminal sexual conduct)], and the difficulty of distinguishing such contexts from all others even in a data warehouse environment may establish practical barriers to Internet access.

Internet access to preconviction criminal records may have significant racial and social implications, and the requirements of Rule 8, subd. 2(c) are intended to minimize the potential impact on persons of color who are disproportionately represented in criminal cases, including in dismissals. The rule contemplates the use of log-ins and other technology that require human interaction to prevent automated information harvesting by software programs. One such technology is referred to as a "Turing test" named after British mathematician Alan Turing. The "test" consists of a small distorted picture of a word and if the viewer can correctly type in the word, access or log in to the system is granted. Right now, software programs do not read clearly enough to identify such pictures. The rule contemplates that the courts will commit resources to staying ahead of technology developments and implementing necessary new barriers to data harvesting off the courts' web site, where feasible.

Some trial courts currently allow public access to records of other courts within their district through any public access terminal located at a court facility in that district. The definition of "remote access" has been drafted to accommodate this practice. The scope of the definition is broad enough to allow statewide access to the records in Rule 8, subd. 2, from any single courthouse terminal in the state, which is the current design of the new trial court computer system referred to as MNCIS.

The exception in Rule 8, subd. 2(e) for allowing remote access to additional documents is intended for individual cases where Internet access to documents will significantly reduce the administrative burdens associated with responding to multiple or voluminous access requests. Examples include high-volume or high-profile cases. The exception is limited to a specific case and does not authorize a standing order that would otherwise swallow the rule.

[Bulk Data Alterntative 1: The 2004 addition of a new Rule 8, subd. 3, on bulk distribution complements the remote access established under the preceding subdivision. The courts have been providing this type of bulk data to the public for the past ten years although its distribution has mainly been limited to noncommercial entities and the media. The bulk data would not include the data elements set forth in Rule 8, subd. 2(b), or any case records that are not accessible to the

public. The bulk data accessible to the public would, however, include preconviction criminal records as Rule 8, subd. 2(c), merely affects the courts' web site display of such records. Concerns over misuse of such information are the province of the legislative branch, which has enacted some measures of protection. *See, e.g.*, the federal Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*, and the Minnesota consumer reports law, MINN. STAT. § 13C.001 *et seq.* (2003).]

[Bulk Data Alterntative 2: The 2004 addition of a new Rule 8, subd. 3, on bulk distribution complements the remote access established under the preceding subdivision. The courts have been providing this type of bulk data to the public for the past ten years although its distribution has mainly been limited to noncommercial entities and the media. The bulk data would include the data elements set forth in Rule 8, subd. 2(b) on any case records that are accessible to the public, including preconviction criminal records. Concerns over misuse of such information are the province of the legislative branch, which has enacted some measures of protection. *See, e.g.*, the federal Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*, and the Minnesota consumer reports law, MINN. STAT. § 13C.001 *et seq.* (2003).]

[Bulk Data Alterntative 3: The 2004 addition of a new Rule 8, subd. 3, on bulk distribution complements the remote access established under the preceding subdivision. The courts have been providing this type of bulk data to the public for the past ten years although its distribution has mainly been limited to noncommercial entities and the media. The bulk data would not include the data elements set forth in Rule 8, subd. 2(b), or any case records that are not accessible to the public. The bulk data accessible to the public would, however, include preconviction criminal records as long as the individual or entity requesting the data enters into an agreement in the form approved by the state court administrator providing that the individual or entity will not disclose or disseminate the data in a manner that identifies specific individuals who are the subject of such data.]

The 2004 addition of new Rule 8, subd. 4, regarding criminal justice and other governmental agencies recognizes that the courts are required to report certain information to other agencies and that the courts are participating in integration efforts (e.g., CriMNet) with other agencies. The access is provided remotely or via regular (e.g., nightly or even annually) bulk data exchanges. The provisions on remote and bulk record access are not intended to affect these interagency disclosures.

The 2004 changes to Rule 8, subd. 5, regarding access to certain evidence is intended to address the situation in which provisions appear to completely cut off public access to a particular document or parts of it even where the item is formally admitted into evidence (i.e., marked as an exhibit and the record indicates that its admission was approved by the court) in a publicly accessible court proceeding. *See, e.g.*, MINN. STAT. § 518.146 (2002) (prohibiting public access to, among other things, tax returns submitted in dissolution cases). The process for formally admitting

evidence provides the opportunity to address privacy interests affected by an evidentiary item. Formal admission into evidence has been the standard for determining when most court services records become accessible to the public under Rule 4, subd. 1(b), and this should apply across the board to documents that are received.

The changes also recognize that evidentiary items may be subject to protective orders or retention schedules or orders. As indicated in Rule 4, subd. 2, and its accompanying advisory committee comment, the procedures for obtaining a protective order are addressed in other rules. Similarly, as indicated in Rule 1, the disposition, retention and return of records and objects is addressed elsewhere.

Rule 9. Appeal from Denial of Access.

If the custodian, other than a judge, denies a request to inspect records, the denial may be appealed in writing to the office of the state court administrator. The state court administrator shall promptly make a determination and forward it ~~by mail~~ in writing to the interested parties as soon as possible. This remedy need not be exhausted before other relief is sought.

Advisory Committee Comment-2004

The 2004 deletion of the term "mail" in Rule 9 recognizes that a determination is often issued in electronic format, such as email or facsimile transmission.

Rule 10. Contracting With Vendors for Information Technology Services.

If a court or court administrator contracts with a vendor to perform information technology related services for the judicial branch: (a) "court records" shall include all recorded information collected, created, received, maintained or disseminated by the vendor in the performance of such services, regardless of physical form or method of storage, excluding any vendor-owned or third-party-licensed intellectual property (trade secrets or copyrighted or patented materials) expressly identified as such in the contract; (b) the vendor shall not, unless expressly authorized in the contract, disclose to any third party court records that are inaccessible to the public under these rules; (c) unless assigned in the contract to the vendor in whole or in part, the court shall remain the custodian of all court records for the purpose of providing public access to publicly accessible court records in accordance with these rules, and the vendor shall provide the court with access to such records for the purpose of complying with the public access requirements of these rules.

Advisory Committee Comment-2004

The 2004 addition of Rule 10 is necessary to ensure the proper protection and use of court records when independent contractors are used to perform information technology related services for the courts. Where the service

involves coding, designing, or developing software or managing a software development project for a court or court administrator, the court or court administrator would typically retain all record custodian responsibilities under these rules and the contract would, among other things: (a) require the vendor to immediately notify the court or court administrator if the vendor receives a request for release of, or access to, court records; (b) prohibit the disclosure of court records that are inaccessible to the public under these rules; (c) specify the uses the vendor may make of the court records; (d) require the vendor to take all reasonable steps to ensure the confidentiality of the court records that are not accessible to the public, including advising all vendor employees who are permitted access to the records of the limitations on use and disclosure; (e) require the vendor, other than a state agency, to indemnify and hold the court or court administrator and its agents harmless from all violations of the contract; (f) provide the court or court administrator with an explicit right to injunctive relief without the necessity of showing actual harm for any violation or threatened violation of the contract; (g) be governed by Minnesota law, without regard to its choice of law provisions; (h) include the consent of the vendor to the personal jurisdiction of the state and federal courts within Minnesota; and (i) require all disputes to be venued in a state or federal court situated within the state of Minnesota.

Rule 11. Immunity.

Absent willful or malicious conduct, the custodian of a record shall be immune from civil liability for conduct relating to the custodian's duties of providing access under these rules.

Advisory Committee Comment-2004

The 2004 addition of Rule 11 is intended to allow record custodians to promptly and effectively discharge their obligations under these rules without undue concern over liability for even one inadvertent error. The burden of redacting each and every reference to specific pieces of information from voluminous records is a daunting task, and the looming threat of liability could turn even the more routine, daily access requests into lengthy processes involving nondisclosure/indemnity agreements. The court has established immunity for records custodians in other contexts. *See, e.g.*, R. BD. JUD. STDS. 3 (members of the board on judicial standards are absolutely immune from suit for all conduct in the course of their official duties); R. LAWYERS PROF. RESP. 21(b) (lawyers professional responsibility board members, other panel members, District Committee members, the Director, and the Director's staff, and those entering agreements with the Director's office to supervise probation are immune from suit for any conduct in the course of their official duties); MINN R. ADMISSION TO THE BAR 12.A. (the Board of Law Examiners and its members, employees and agents are immune from civil liability for conduct and communications relating to their duties under the Rules of Admission to the Bar or the Board's policies and procedures); MINN. R. BD. LEGAL CERT. 120 (the Board of Legal Certification and its members, employees, and agents are immune from civil liability for any acts conducted in the course of their official duties); MINN. R. CLIENT SEC. BD. 1.05 (the Client Security Board and its

staff are absolutely immune from civil liability for all acts in the course of their official capacity). Rule 11 does not, however, avoid an administrative appeal of a denial of access under Rule 9, declaratory judgment, writ of mandamus, or other similar relief that may otherwise be available for a violation of these rules.

APPENDIX A

Boards and Commissions that are governed by independent rules promulgated by the Supreme Court include, but are not limited to, the following:

Lawyers Professional Responsibility Board
Lawyer Trust Account Board
Client Security Fund Board
State Board of Legal Certification
Board of Continuing Education
State Board of Law Examiners
State Bar Advisory Council
Board on Judicial Standards
Standing Committee on No Fault Arbitration
Legal Services Advisory Committee

~~APPENDIX B~~

~~Statutes making certain case records inaccessible to the public include, but are not limited to, the following:~~

~~Minnesota Statute~~	~~Type of Record or Proceeding~~
~~144.343, subd. 6~~	~~Abortion notification proceedings~~
~~144.218, subd. 2; 259.27; 259.31; 259.49; 260.161~~	~~Adoption proceedings~~
~~257.56~~	~~Artificial insemination~~
~~253B.23, subd. 9~~	~~Commitments~~
~~254.09~~	~~Compulsory treatment~~
~~626A.06, subd. 9~~	~~Wiretap warrants~~
~~609.3471~~	~~Identity of juvenile victims of sexual assault~~
~~609.115~~	~~Presentence investigation report~~
~~169.126~~	~~Alcohol problem assessment report~~
~~638.02~~	~~Pardon~~
~~242.31; 152.18 subds. 1,2,3~~	~~Expunged records~~

~~518.168(d) Custody proceedings~~
~~260.161 Juvenile court records~~
~~257.70 Paternity proceedings~~
~~525.22 Wills deposited for safekeeping~~

APPENDIX C

State and federal laws making certain administrative records inaccessible to the public include, but are not limited to, the following:

Citation*	Type of Record
M.S. §§ 593.42, subd. 5; 593.47	Jury data
22 C.F.R. § 51.33	Passport records
M.S. § 260.195, subd. 6	Juvenile placements
M.S. §§ 626A.06, subd. 9; 626A.17	Report of wiretap warrants
Rule 9, R. Reg. Attorneys	Registered Attorneys Mailing List
Rule 5, R. Jud. Ed.	Supreme Court Continuing Education Office records

*M.S. denotes Minnesota Statutes; C.F.R. denotes the Code of Federal Regulations; R. Reg. Attorneys denotes Rules of the Supreme Court for Registration of Attorneys, amended by Supreme Court Order dated Feb. 13, 1986; R. Jud. Ed. denotes Rules of the Supreme Court for Judicial Education of Members of the Judiciary, promulgated pursuant to Supreme Court Order dated Oct. 11, 1979.

APPENDIX D

The following statutes and regulations issued pursuant to statute, govern the accessibility of vital statistics records:

Citation*	Type of Record
M.S. §§ 144.218; 144.1761; 144.216; 257.73	Original birth certificate prior to: adoption of child; marriage of natural parents; acknowledgement or adjudication of paternity; and filing of corrected certificate.
M.S. § 144.225; M.R. 4600.6000	Birth certificates and marriage license applications disclosing child born out ofwedlock
M.R. 4600.5800	Birth and death certificates; commercial use.

*M.S. denotes Minnesota Statutes; M.R. denotes Minnesota Rules, which is a compilation of rules promulgated by agencies in the executive branch.

Exhibit B: Proposed Amendments to Rules of Civil Procedure

Rule 47.01 Examination of Jurors

The court may permit the parties or their attorneys to conduct the examination of prospective jurors or may itself conduct the examination. In the latter event, the court shall permit the parties or their attorneys to supplement the examination by such further inquiry as it deems proper. Supplemental juror questionnaires completed by jurors shall not be accessible to the public unless formally admitted into evidence in a publicly accessible hearing or trial.

Advisory Committee Comment-2004 Amendments

The addition of the last sentence in Rule 47.01 precluding public access to completed supplemental juror questionnaires recognizes both the legitimate privacy interests of jurors and the interests of the public in otherwise publicly accessible court proceedings. This rule does not apply to juror qualification questionnaires submitted by jurors pursuant to MINN GEN. R. PRAC. 807; public access to completed qualification questionnaires is governed by MINN. GEN. R. PRAC. 814.

Exhibit C: Proposed Amendments to General Rules of Practice, Rule 814

RULE 814. RECORDS

The names of qualified prospective jurors drawn and the contents of completed juror qualification questionnaires shall not be disclosed except as provided by this rule or as required by Rule 813.

(a) **Qualified public access.** Prior to the expiration of the time period in part (d) of this rule, t~~T~~he names of qualified prospective jurors drawn and the contents of juror qualification questionnaires, except social security numbers, completed by those prospective jurors must be made available to the public upon specific request to the court, supported by affidavit setting forth the reasons for the request, unless the court determines:

(1) in a criminal case~~any instance~~ that access to any such information should be restricted pursuant to Minn. R. Crim. P. 26.02, subd. 2(2);

(2) in all other cases that in the interest of justice this information should be kept confidential or its use limited in whole or in part.

(b) **Limits on Access by Parties.** The contents of completed juror qualification questionnaires except juror social security numbers must be made available to lawyers upon request in advance of voir dire. The court in a criminal case may restrict access to names, telephone numbers, addresses and other identifying information of the ~~prospective~~ jurors only as permitted by Minn. R. Crim. P. 26.02, subd. 2(2). In a civil case the court may restrict access to the names, addresses, telephone numbers and other identifying information of the jurors in the interests of justice.

(c) **Retention.** The jury commissioner shall make sure that all records and lists are preserved for the length of time ordered by the court.

(d) **Unqualified Public Access.** After ~~The contents of any records or lists not made public shall not be disclosed until~~ one year has elapsed since preparation of the list and all persons selected to serve have been discharged, the contents of any records or lists, except identifying information to which access is restricted by court order and social security numbers, shall be accessible to the public. ~~unless a motion is brought under Rule 813.~~

Advisory Committee Comment—2004 Amendment

Rule 814 has been modified in 2004 to ensure the privacy of juror social security numbers and to reflect the constitutional limits on closure of criminal case records. Juror qualification records on a particular juror will be subject to those constitutional limits only to the extent that the juror has participated in voir dire in a criminal case. Access to completed supplemental juror questionnaires used in specific cases is governed by separate rules. *See* MINN. R. CIV. P. 47.01; MINN. R. CRIM. P. 26.02, subd. 2(3).

Exhibit D: Proposed Amendments to General Rules of Practice,
Rules 103, 313, 355

RULE 103 SUBMISSION OF CONFIDENTIAL NUMBERS

The requirements set forth in Rule 313.02 of these rules for submitting restricted identifiers, such as social security numbers and financial account numbers, shall apply to all civil cases.

RULE 313. CONFIDENTIAL NUMBERS AND TAX RETURNS

Rule 313.01. Definitions. For purposes of this rule, the following definitions shall apply:

(a) "Restricted identifiers" shall mean the social security number [and/or employer identification number] and financial account numbers of a party or party's child.

(b) "Financial source documents" means income tax returns, W-2s and schedules, wage stubs, credit card statements, financial institution statements, check registers, and other financial information deemed financial source documents by court order.

Rule 313.0~~1~~2. ~~Social Security Number~~Restricted Identifiers.

(a) **Pleadings and Other Papers Submitted by a Party**. No party shall submit restricted identifiers~~Whenever an individual's social security number is required~~ on any pleading or other paper that is to be filed with the court except~~, the social security number shall be submitted~~

(i) on a separate form entitled Confidential Information Form (see Form 11 appended to these rules) filed with the pleading or other paper; or

(ii) on Sealed Financial Source Documents under Rule 313.03.

The parties are solely responsible for ensuring that restricted identifiers do ~~and shall~~ not otherwise appear on the pleading or other paper filed with the court. The court administrator will not review each pleading or document filed by a party for compliance with this rule. The Confidential Information Form shall not be accessible to the public.

(b) **Records Generated by the Court**. Restricted identifiers maintained by the court in its register of actions (i.e., activity summary or similar information that lists the title, origination, activities, proceedings and filings in each case), calendars, indexes, and judgment docket shall not be accessible to the public. Courts shall not include

restricted identifiers on their judgments, orders, decisions, and notices except on the Confidential Information Form (Form 11), which form shall not be accessible to the public. ~~As an alternative, the filing party may prepare and file an original and one copy of the pleading or other paper if all social security numbers are completely removed or obliterated from the copy.~~

Rule 313.0~~2~~3. Sealing Financial Source Documents ~~Tax Returns~~.

~~Copies of tax returns required to be filed with the court shall be submitted in a separate envelope marked "CONFIDENTIAL TAX RETURN OF _____ for YEAR(S) _____."~~ Financial source documents shall be submitted to the court for filing under a cover sheet designated "Sealed Financial Source Documents" and substantially in the form set forth as Form 12 appended to these rules. Financial source documents submitted with the required cover sheet are not accessible to the public except to the extent that they are formally admitted into evidence in a hearing or trial. The cover sheet or copy of it shall be accessible to the public. Financial source documents that are not submitted with the required cover sheet and that contain restricted identifiers are accessible to the public, but the court may, upon motion or on its own initiative, order that any such financial source documents be sealed.

Rule 313.0~~3~~4. Failure to comply.

~~A~~ If a party ~~who~~ fails to comply with the requirements of this rule in regard to another individual's restricted identifiers or financial source documents, ~~may be deemed to have waived their right to privacy in their social security number or tax return filed with the court and~~ the court may upon motion or its own initiative impose appropriate sanctions, including costs necessary to prepare an appropriate document for filing ~~redacted copy, for a party's failure to comply with this rule in regard to another individual's social security number or tax return~~.

Rule 313.05 Procedure for Requesting Access to Sealed Financial Source Documents.

(a) Motion. Any person may file a motion, supported by affidavit showing good cause, for access to Sealed Financial Source Documents or portions of the documents. Written notice of the motion shall be required.

(b) Waiver of Notice. If the person seeking access cannot locate a party to provide the notice required under this rule, after making good faith reasonable effort to provide such notice as required by applicable court rules, an affidavit may be filed with the court setting forth the efforts to locate the party and requesting waiver of the notice provisions of this rule. The court may waive the notice requirement of this rule if the court finds that further good faith efforts to locate the party are not likely to be successful.

(c) Balancing Test. The court shall allow access to Sealed Financial Source Documents, or relevant portions of the documents, if the court finds that the public interest in granting access or the personal interest of the person seeking access outweighs

the privacy interests of the parties or dependent children. In granting access the court may impose conditions necessary to balance the interests consistent with this rule.

* * *

Advisory Committee Comment—2004 Amendment

Rule 313 is completely revised in 2004 based on WASH. R. GEN. GR 22 (2003). Parties are now responsible for protecting the privacy of restricted identifiers (social security numbers [and/or employer identification numbers] and financial account numbers) and financial source documents by submitting them with the proper forms. Failure to do so means that the public will be able to access the numbers and documents from the case file unless the party files a motion to seal them under Rule 313.03 or 313.04. The Confidential Information Form is retained and modified, and a new Sealed Financial Source Document cover sheet has been added. Also retained is the authority of the court to impose sanctions against parties who violate the rule in regard to another individual's restricted identifiers or financial source documents.

New in 2004 is the procedure for obtaining access to restricted identifiers and sealed financial source documents. This process requires the court to balance the competing interest involved. *See, e.g., Minneapolis Star & Tribune v. Schumacher*, 392 N.W.2d 197 (Minn. 1986) (when party seeks to restrict access to settlement documents and transcripts of settlement hearings made part of civil court file by statute, court must balance interests favoring access, along with presumption in favor of access, against those asserted for restricting access).

Rule 355.05. Filing of Pleadings, Motions, Notices and Other Papers.

* * *

Subd. 5. Confidential Numbers and Tax Returns. The requirements of Rule 313 of these rules regarding submission of restricted identifiers (e.g., social security numbers~~,~~ [and/or employer identification numbers,] financial account number) and financial source documents (e.g., tax returns, wage stubs, credit card statements) shall apply to the expedited child support process.

FORM 11. CONFIDENTIAL INFORMATION FORM (Gen. R. Prac. 313.0~~1~~2; 103)

State of Minnesota **District Court**

County of _____ **_____Judicial District**

Case Type:

Case No. _____

_____
Plaintiff/Petitioner

and

CONFIDENTIAL INFORMATION FORM

(Provided Pursuant to Rules 313.0~~1~~2 and 103 of the Minnesota General Rules of Practice)

_____
Defendant/Respondent

The information on this form is confidential and shall not be placed in a publicly accessible portion of a file.

		NAME	SOCIAL SECURITY NUMBER [EMPLOYER IDENTIFICATION NUMBER] AND FINANCIAL ACCOUNT NUMBERS
Plaintiff/Petitioner	1.		
	2.		
	3.		
Defendant/	1.		
Respondent	2.		
	3.		
Other Party (e.g.,	1.		

minor children) _____

2. _____ _____

_____

Information supplied by:

_____

(print or type name of party submitting this form to the court)

Signed: _____

Attorney Reg. #: _____

Firm: _____

Address: _____

_____

Date: _____

FORM 12. SEALED FINANCIAL SOURCE DOCUMENTS (Gen. R. Prac. 313.02)

State of Minnesota **District Court**

County of _____ **_____Judicial District**

Case Type:

Case No. _____

_____
Plaintiff/Petitioner

and **SEALED FINANCIAL SOURCE DOCUMENTS** (Provided Pursuant to Rule 313.02 of the Minnesota General Rules of Practice)

_____
Defendant/Respondent

THIS LISTING OF SEALED FINANCIAL SOURCE DOCUMENTS IS ACCESSIBLE TO THE PUBLIC BUT THE SOURCE DOCUMENTS SHALL NOT BE ACCESSIBLE TO THE PUBLIC EXCEPT AS AUTHORIZED BY COURT RULE OR ORDER

? Income tax records
Period covered:

? Bank statements
Period covered:

? Pay stubs
Period covered:

? Credit Card statement
Period covered:

? Other:

Information supplied by:

_____
(print or type name of party submitting this form to the court)

Signed: _____

Attorney Reg. #: _____

Firm: _____

Address: _____

_____

Date: _____

Exhibit E: Race Census Form

Name _____ Case/File number _____

RACE CENSUS FORM

The Minnesota Courts are collecting information on all people who appear in criminal, traffic and juvenile cases. Collecting this information will help the Court ensure that everyone is treated fairly and equally, regardless of his/her race or ethnicity.

Please answer **both** questions 1 and 2 below.

1. What is your race?

Mark an **X** by one or more races to indicate what race you consider yourself to be.

_____ (I). American Indian or Alaska Native

_____ (A). Asian

_____ (B). Black or African American

_____ (H). Native Hawaiian or Other Pacific Islander

_____ (W). White

_____ (O). Other:_____

2. Are you Hispanic or Latino?

Mark the "NO" box if not Hispanic or Latino

_____ (N). **NO**, Not Hispanic or Latino

_____ (Y). **YES,** Hispanic or Latino

Have you answered **both** questions?
For definitions see the back of this form.

Definitions:

Race Categories: *

American Indian or Alaska Native: A person having origins in any of the original peoples of North and South America (including Central America), and who maintains tribal affiliation or community attachment.

Asian: A person having origins in any of the original peoples of the Far East, Southeast Asia, or the Indian subcontinent including, for example, Cambodia, China, India, Hmong, Japan, Korea, Malaysia, Pakistan, the Philippine Islands, Thailand, and Vietnam.

Black or African American: A person having origins in any of the black racial groups of Africa, for example Somalia. Terms such as "Haitian" can be used in addition to "Black or African American."

Native Hawaiian or Other Pacific Islander: A person having origins in any of the original peoples of Hawaii, Guam, Samoa, or other Pacific Islands.

White: A person having origins in any of the original peoples of Europe, the Middle East, North Africa, or Mexico.

Ethnicity: *

Hispanic or Latino: A person of Cuban, Mexican, Puerto Rican, South or Central American, or other Spanish culture or origin, regardless of race. The term, "Spanish origin," can be used in addition to "Hispanic or Latino."

* The United States Census Bureau has established these Race and Ethnicity categories

Exhibit F: Members of Minnesota Supreme Court Advisory Committee on the Rules of Public Access to Records of the Judicial Branch

Hon. Paul H. Anderson
Minnesota Supreme Court
St. Paul

Mark R. Anfinson
Attorney at Law
Minneapolis

Donna Bergsgaard
Thomson West
Eagan

Van Brostrom
District Court Administrator
Hastings

Sue K. Dosal
State Court Administrator
St. Paul

Hon. Kathleen R. Gearin
Ramsey County District Court
St. Paul

Donald A. Gemberling
Public Information Policy Analysis,
Dept. of Administration
St. Paul

Paul R. Hannah
Attorney at Law
St. Paul

Hon. Natalie Hudson
Minnesota Court of Appeals
St. Paul

Hon. Timothy J. McManus
Dakota County District Court
Hastings

Gene Merriam
Commissioner, Minnesota Department
of Natural Resources
St. Paul

Jane F. Morrow
District Court Administrator
Anoka

Teresa Nelson
Minnesota Civil Liberties Union
St. Paul

Pamela McCabe
Anoka County Attorney's Office
Anoka

Hon. John R. Rodenberg
Brown County District Court
New Ulm

Hon. Warren Sagstuen
Hennepin County District Court
Minneapolis

Robert Sykora
Minnesota Board of Public Defense
Minneapolis

Lolita Ulloa
Office of Hennepin County Attorney
Victim/Witness Assistance Program
Minneapolis

Gary A. Weissman
Weissman Law Office
Minneapolis

Exhibit G: Minority Report - Family Law Records

Adult citizens are free to rescind contracts into which they enter voluntarily, without court supervision. The one exception is a marriage contract whose dissolution the law requires be approved by a judge and recorded in a court file.

That the marriage was dissolved and that the court has awarded real property to one of them should be public information (and there are extant statutes which allow these narrowly drawn items to be filed shorn of other, personal data).[114] Divulging other information about the divorcing couple, their children, and their finances, however, serves no public policy purpose.

Untroubled by the unequal protection afforded to married people (as opposed to unmarried parents, whose battles over paternity, custody, and child support are protected from disclosure by statute),[115] the majority of the advisory committee concluded that the public disclosure of parental access schedules, the incomes of the parties, the amounts of child support and spousal maintenance, and the extent of the parties' investments is a reasonable concomitant of divorce.

Because the advisory committee disavows accountability for documents not generated by the court, technology will soon enable anyone with access to the internet to read the undiluted hyperbole of affidavits filed in marriage dissolutions as well as filed reports from psychologists, custody evaluators, guardians-ad-Litem, parenting time expediters, accountants, vocational evaluators, actuaries, and property appraisers, irrespective of either the veracity of the data or the appropriateness of public disclosure.

Such policies validate gross intrusions on personal privacy and constitute an unwarranted marriage penalty.

Even though the majority supports keeping these records public, the rich, the powerful, and those "in-the-know" already have a privacy remedy, namely, sealing their files. We propose, at a minimum, that court procedures (and these rules) provide

[114] MINN. STAT. § 518.148 (2002) permits the creation of a Certificate of Dissolution, which discloses only that and when the parties were divorced. MINN. STAT. § 518.191 authorizes a Summary Real Estate Disposition Judgment to convey real property awarded in a divorce without revealing other personal information.

[115] MINN. STAT. § 257.70 (2002).

notice to all family law litigants of the availability of the right to seal their case records.

-- Gary A. Weissman
-- Donald A. Gemberling

Exhibit H: Minority Report: Fair Information Practices

In focusing most of its attention on electronic access to court records, the advisory committee missed a vital opportunity to institute any of the Fair Information Practices principles:[116]

TOPIC HEADING	PRINCIPLE
1. Anti-secrecy	There must be no personal data record-keeping systems whose very existence is secret.
2. Individual access	There must be a way for individuals to find out what information about them is in a record and how that information is used.
3. Limited secondary disclosure	There must be a way for individuals to prevent information about them obtained for one purpose from being used or made available for other purposes without their consent.
4. Correcting errors	There must be a way for individuals to correct or amend a record of identifiable information about them.
5. Reliability	Any entity creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of those data.

All of these principles inhere in obligations imposed by the Data Practices Act on cities, on counties, on school districts, and on the executive branch of state government; but none will attach to the judicial branch if the Supreme Court adopts the recommendations of the advisory committee.

[116] The 1973 federal task force, the HEW Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens*, identified five fair information practice principles. Those five principles informed much of the content of both the Federal Privacy Act and the Minnesota Government Data Practices Act.

The 1986 advisory committee, whose work product comprises the current Rules of Public Access to Records of the Judicial Branch, limited its scope to accessibility and made no mention of the rights of individuals. The 2003 advisory committee, regretfully, proposes rules which ignore individual access, which omit provisions for limiting secondary disclosure, which provide impracticable remedies for correcting errors, and which decline accountability for unreliability.

The committee's recommendations only marginally seek to protect individual privacy, limiting that protection to social security numbers, tax records, and crime victim information. Even that protection is toothless, however, because of a lack of viable redress for its violation.

The federal task force in the early 1970s looked into the future to minimize the adverse impact of automation on individual human beings. Minnesota's advisory committee, unfortunately, frames the problem as how to minimize the impact on court administrators. The proposed rules are a 20th century solution to a 21st century situation, where courts are no longer mere repositories of records but are, for better or worse, purveyors of valuable information.

-- Donald A. Gemberling
-- Gary A. Weissman

Exhibit I: Bulk Data Alternative 1

By a vote of 11 to 3, the advisory committee recommends that any court records that are accessible to the public on the Internet (discussed above) should be accessible to the public in bulk format. This recommendation is set forth in proposed ACCESS RULE 8, subd. 3 Bulk Data Alternative 1 (see Exhibit A, attached to this report). Thus, the recommendation to preclude public access to personal identifiers on the Internet will also preclude public access to personal identifiers in bulk record disclosures. Preconviction criminal records, however, are not completely off limits to the public on the Internet; the committee's recommendation only prohibits these records from being searchable via the Internet by automated means. For example, a calendar containing unproven criminal allegations would be accessible via the Internet if it is presented using certain log-ins, file formats and file names. Thus, a member of the public would still have Internet access to the record under the recommended rule. Therefore, bulk disclosures would include unproven criminal accusations.[117]

At first glance, some may see this as an about face as it appears to render the Internet access limitations moot; commercial data brokers will simply take the bulk preconviction records and make them available online as they do now with paper records. Proponents, however, see a distinction between access by commercial data brokers who will pay fees (discussed on page 23) for bulk data and then sell the data

[117] A subset of the advisory committee believes that bulk preconviction records should only be made accessible to recipients who agree to limit their dissemination of preconviction records to aggregate form (i.e., does not identify individuals associated with a particular preconviction record). *See* Exhibit K supporting Bulk Data Alterntative 3. Those supporting Bulk Data Alternative 3 grossly mischaracterize Bulk Data Alternative 1 when they claim that the supporters of Bulk Data Alternative 1 assert "that the relatively few overall criminal cases involving the falsely or mistakenly charged simply do not outweigh the significant benefit of Internet access." See Exhibit K at page 85 (the mischaracterization is essentially repeated in different words on page 89). As the discussion above indicates, this assertion was made by only a few members of the committee, and it was made by those in the minority on a separate issue (i.e., Internet access, see pages 16-17 of this report). Those supporting Bulk Data Alternative 3 also claim that data entry problems in the Fourth Judicial District result in errors in attorney names in that district's SIP computer system. *See* Exhibit K at pages 86-88. Those supporting Bulk Data Alternative 3 acknowledge that these data quality problems found on the Fourth Judicial District site are not duplicated on the Minnesota Supreme Court attorney registration site. *Id.* What they leave out is that the SIP system is being phased out over the next year and its replacement (i.e., the MNCIS system) uses the attorney registration database as its source for attorney information.

to the public, and access by the general public to all preconviction records from the court's web site. Information provided by commercial data brokers lacks the imprimatur of the court,[118] and commercial enterprises are also more likely to come under one or more laws that regulate use of consumer information.[119]

Bulk Data Alternative 1 will not prevent the Minnesota Supreme Court from authorizing disclosure of a wider range of bulk data by court order when necessary and appropriate (e.g., to educational or research institutions such as the National Center for Juvenile Justice).

[118] This point was made by a number of commentators at the public hearing. *See, e.g.*, public hearing comments of John Stuart, State Public Defender; public hearing comments of Kizzy Johnson, Communities Against Police Brutality; public hearing comments of Scott Benson and Don Samuels, Minneapolis City Council Members.

[119] *See, e.g.*, the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*., the Gramm-Leach- Bliley Act, 15 U.S.C. 6801 *et seq*., and the Minnesota credit reporting law, MINN. STAT. §§ 13C.001-.04 (2003). The Consumer Data Industry Association urged the committee to go even farther and allow bulk data disclosures of the full social security numbers in court records to certain qualified users like consumer reporting agencies and other entities that conform to such laws. Letter from Eric Ellman, Director and Counsel, Government Relations, Consumer Data Industry Association, to Michael Johnson, advisory committee staff, undated. The committee was unable to find a jurisdiction that had implemented such a process.

Exhibit J: Bulk Data Alternative 2

Bulk Data Alternative 1 limits the ability of the public to receive bulk distribution of electronic case records:

> ***Subd. 3. Bulk Distribution of Electronic Case Records.*** *A court administrative office shall provide bulk distribution of only its electronic case records that are remotely accessible to the public pursuant to subdivision 2 of this rule, to the extent that office has the resources and technical capacity to do so. "Bulk distribution" means distribution of all, or a significant subset, of the court's electronic case records.*

This provision is quite different from the recommendation of the Data Policy Subcommittee of the Technology Planning Committee, which states:

> ***Section 4.30 - Requests for Bulk Distribution of Court Records***
>
> *Bulk distribution is defined as the distribution of all, or a significant subset, of the information in court records, as is and without modification or compilation.*
>
> > *(a) Bulk distribution of information in the court record is permitted for court records that are publicly accessible under section 4.10.*
> >
> > *(b) A request for bulk distribution of information not publicly accessible can be made to the court for scholarly, journalistic, political, governmental, research, evaluation or statistical purposes where the identification of specific individuals is ancillary to the purpose of the inquiry. Prior to the release of information pursuant to this subsection the requestor must comply with the provisions of section 4.40(c).*

The Committee should understand that refusing to grant access to bulk data render those data non-public, as a practical matter. Many publicly beneficial uses of the data cannot be accomplished with access to individual files. Some Committee members believe that this restrictive access rule will keep these data from being disseminated on the internet, but data "harvesters" will still have access, and will still disseminate the data.

Refusing to allow access to bulk data stored in electronic form goes against the common law rule of access to court data. "It is undisputed that a common law right to inspect and copy civil court records exists." *Minneapolis Star & Tribune v. Schumacher*, 392 N.W.2d 197, 202 (Minn. 1986), citing, *inter alia*, *Nixon v. Warner Communications, Inc.*, 435 U.S. 589, 597 (1977). The right to inspect and copy records is considered "fundamental to a democratic state." *United States v. Mitchell*, 551 F.2d 1252, 1258 (D.D.C. 1976).

There is a constitutional dimension to access to court data. *See, e.g*. *Richmond Newspaper, Inc. v. Virginia*, 448 U.S. 555 (1980); *Gannett Co. v. De Pasquale*, 443 U.S. 368 (1979). Bulk Data Alternative 1's shielding of these data would never survive the strict scrutiny standard which courts apply to such restrictions.

Committee members accepted Bulk Data Alternative 1 because of concerns over the possible "misuse" of those data. However, provisions which restrict access to otherwise public data based on the manner of use of that data would never withstand court applied "strict scrutiny" or "balancing of the interests" tests. For example, a party seeking to restrict the common law right of access to court records must assert "strong countervailing reasons" to overcome the presumption of openness. *Schumacher*, 392 N.W.2d at 205-206. Bulk Data Alternative 1 does not satisfy this test.

While Committee members may believe that Bulk Data Alternative 1 somehow protects personal privacy, that belief is illusory. These data, if valuable, will ultimately be "harvested" in a number of ways by those seeking a financial reward. Ultimately, there is no real privacy protection when the data in question are public.

In fact, while the value of the data will convince data "harvesters" to take measures to gain access to the data, the provision will dramatically limit the use of such data for research purposes, and for public accountability. A rapidly growing area of journalism practice involves computer-assisted reporting. Access to databases allows the media, academics and others to make comparisons and connections to data that would never be available if the researcher were forced to look through the files on an individual basis. While a data "harvester" with a profit incentive may make several trips to the courthouse for the data, journalists or researchers may not have those resources available.

Moreover, the kinds of stories that might be written with access to these databases are never as compelling when they are based only on "summary" data. In fact, many of the stories which are based on comparison of databases improve their impact because they include individual stories, which are possible only when the identity of the data subjects are known.

CONCLUSION

We do not believe Bulk Data Alternative 1 as presently drafted will provide substantial protection to otherwise public data. We do not believe Bulk Data Alternative 1 will prevent the otherwise public data from being "harvested."

If, ultimately, Bulk Data Alternative 1 does not prevent the data from being used by "harvesters," then this Committee is severely limiting beneficial public access without actually providing any substantive privacy protection.

For these reasons, we propose that Section 4.30 "Requests for Bulk Distribution of Court Records" from the Guidelines be substituted for Bulk Data Alternative 1.

- Paul R. Hannah
- Gary A. Weissman

Exhibit K: Report Supporting Restrictions on
Bulk Distribution of Court Data (Bulk Data Alternative 3)

OVERVIEW

After more than a year of thoughtful work, the advisory committee has made a distinction between the court data that is to be disseminated via *the courts' own web sites* and the data *distributed to bulk data harvesters*. The majority correctly recommends to the Minnesota Supreme Court that it restrict accessibility of preconviction criminal data via its own web sites. Bulk Data Alternative 1 also recommends that private data harvesters be allowed to obtain from our court system data about unproven accusations about individuals and disseminate that information in bulk format without restriction. The signers to this report believe Bulk Data Alternative 1 to be a mistake.

Instead, we recommend that the Minnesota Supreme Court adopt a policy allowing bulk distribution of data only to recipients who agree not to disseminate preconviction personal identifying data to third parties.[120] We believe: (1) the unfettered distribution of preconviction criminal data compromises the presumption of innocence; and, (2) the Minnesota Supreme Court should be confident that the data to be distributed have been proven accurate, complete and reliable.

The Minnesota Supreme Court can strike a balance between individual rights and the public's right to know by allowing access to bulk information and restricting downstream dissemination of personal identifying information in preconviction criminal matters.

This report will demonstrate why the data at issue are unreliable, discuss the presumption of innocence and the racially disparate impact of the majority's scheme for data dissemination, and offer an alternative that will protect the rights of individuals who have been charged but not convicted.

THE CONSTITUTION DOES NOT TOLERATE "RELATIVELY FEW" ABROGATIONS OF THE PRESUMPTION OF INNOCENCE

The Committee has been mindful of the Constitutional mandate to preserve the presumption of innocence as it has carefully developed the set of rules it now recommends for Minnesota Supreme Court adoption. Indeed, the committee has been

[120] Bulk Data Alternative 3 set forth in Exhibit A, at Rule 8, subd. 3, contains proposed language which would both allow openness and restrict downstream dissemination of personal identifiers in preconviction criminal matters.

very careful to provide protections that affect how the court's own web site operates, in stark contradiction to the unfettered access to preconviction data that it provides to bulk data harvesters

Those who support Bulk Data Alternative 1 recommend that the court take two seemingly inconsistent actions: on one hand, it recommends that the court's own web site managers take steps to discourage bulk harvesting of data and using names to search preconviction data; on the other hand, it recommends that bulk data be provided to data harvesters who will do exactly that.

This recommendation is predicated on the correct understanding that data harvesters handle data differently than does the general public. For example, a reference-checking service is more likely to disclose its sources to the data subject because of the Fair Credit Reporting Act, unlike a landlord or employer who is much less likely to abide by this principle of fairness.

Rational or not, however, the recommendation is faulty because it does not fully preserve the presumption of innocence.

Those supporting Bulk Data Alternative 1 assert that "[t]he relatively few overall criminal cases involving the falsely or mistakenly charged simply do not outweigh the significant benefit of Internet access" (and, presumably, the unrestrained bulk data dissemination recommended by the majority). But the Constitution has no exception allowing "relatively few" violations of the presumption of innocence. It is not a principle that can be compromised in favor of expediency and convenience. It is a "bedrock axiomatic and elementary principle whose enforcement lies at the foundation of the administration of our criminal law." *In re Winship*, 397 U.S. 358, 363 (1970) (internal quotations omitted). (cited with approval by Minnesota Supreme Court in *State vs. Dwane David Peterson*, 673 N.W.2d 482 (Minn. 2004)).

THE COURT SYSTEM SHOULD NOT DISSEMINATE BULK DATA WITHOUT RESTRICTION WHEN THE COURT CANNOT BE REASONABLY CERTAIN THE DATA ARE ACCURATE. CURRENT PRACTICE SUGGESTS THAT THESE DATA WILL NOT BE SUFFICIENTLY ACCURATE

The advisory committee's report only obliquely addresses problems the court system has with the accuracy of its data. The report acknowledges that "the advent of Internet publication will significantly magnify the potential for harm that such errors can cause," and then provides for error correction procedures when mistakes are located. But the committee did not consider the extent of the problem, perhaps

because no one knows just how bad the problem might be. The committee saw no accuracy and completeness audits of courtroom data, if such audits exist.

The court's record management system relies on courtroom clerks to enter data. This is one responsibility among many for clerks who each day work under a great amount of pressure. Moreover, in most Minnesota courtrooms, data are not entered in real-time. Instead, most clerks enter the information into the court's records management system later, transcribing from notes taken during the hearing. The committee is aware of no formal assessment or audit of the quality of the data entered by courtroom clerks. In addition, the court is transitioning to a new computer system with the hope that its design will improve accuracy, but no proof yet exists on this point.

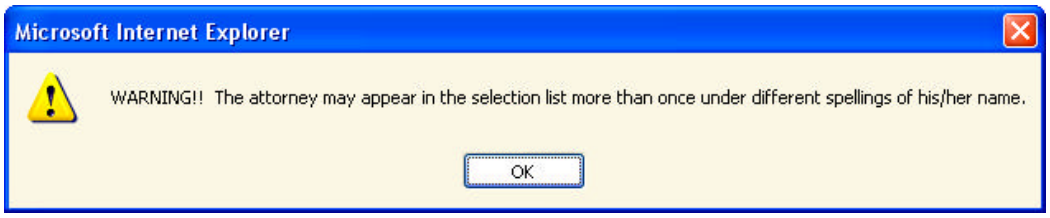
In the absence of clear answers to these questions, consider the experience of Hennepin County courts, long the state's leading jurisdiction in the use of computers to capture and manage court-related data, as it attempts to provide accurate court data on the Internet via its Subject in Process (SIP) databases, which are different than those used in other Minnesota courtrooms.

Example of inability to provide reliable court data on the Internet

In May 2004, Hennepin County Courts provided court data at this web address: **http://www2.co.hennepin.mn.us/dccalendar/criteria.jsp**

This online resource is designed to allow court staff, lawyers, and parties Internet access to calendars. The web page has a "drop-down" box which can be used to select the attorney name, and all of the cases in which the selected attorney is appearing as counsel. The screen looks like this:

A quick look at the list of attorneys reveals that it is compromised by severe data integrity problems. There are many near-duplicate names, apparently caused by data entry errors. Also, there are misspellings and apparent confusion about whether the names should be listed last name first or first name first. Hennepin County is aware of the integrity problem, presenting the following warning to users attempting to search by attorney name:



In fact, of the 779 defense attorney names listed in April 2004, 336 names – *half* – showed one of the inaccuracies listed above.

Practically speaking, this means that if you want to see all cases calendared for Kenneth Bottema and Hersch Izek, you must make separate searches under all of the following names:

- Bottema, Kenneth
- Bottema, Ken
- Botema, Ken
- Ken Bottema
- Ken Bottems
- Kenneth Botema
- Kenneth Bottema
- Kenneth M Bottema
- Hersch Izak
- Hersch Izek
- Isaac, Hersch
- Isak, Hersch
- Isaak, Hersch
- Izak, Hersch
- Izak, Hersh
- Izek, Hersch
- Izek, Hersh

Users seeking cases for Anthony Torres will not find them under A or T: Mr. Torres is listed only as J Anthony Torres.

The population of defense attorneys in Hennepin County is a discrete and fairly well known group of individuals. Each one of them is clearly identified by a unique attorney registration number assigned by the Minnesota Supreme Court.[121] **If the Hennepin County courts – after three decades of experience with computer-based court records – cannot keep accurate records of 779 defense attorneys, it is not reasonable for us to expect that the very same data entry clerks will be able to maintain an accurate record of the tens of thousands of defendants appearing in the same court.** Defendants routinely use alias names, confusing recordkeeping tremendously. Only a small subset of defendants, those who have previous convictions for serious offenses, are fingerprinted and assigned a state identification number. Those accused of most misdemeanors, the vast bulk of the court's caseload, are not. Courtrooms are busy places and clerks are overworked.

Data quality problems like this are not unique to the courts. Gartner, Inc., a major provider of research and analysis on the global information technology industry, estimates that more than 25 percent of critical data within Fortune 1,000 businesses is inaccurate or incomplete.[122] Given that data entry inaccuracies prevent a trial court system from reliably tracking a comparatively small number of attorneys, it is unreasonable to expect it to be reliable when recording information about vastly greater numbers of litigants.

DISPROPORTIONATE RACIAL IMPACT

The advisory committee acknowledges disproportionate impact of the criminal justice system upon ethnic and racial minorities, and suggests that Internet posting of preconviction criminal information helps society to become aware of such problems

[121] Note that these data quality problems found on the Hennepin site are not duplicated on the Supreme court attorney registration site, found at http://www.courts.state.mn.us/mars/default.aspx

[122] *Using Business Intelligence to Gain a Competitive Edge: Unleashing the Power of Data Analysis to Boost Corporate Performance*, April 2004, Gartner, Inc. *See* http://www4.gartner.com/5_about/press_releases/asset_74687_11.jsp

and to address them. But the Minnesota Supreme Court could easily make bulk preconviction criminal information available for such laudable public policy purposes while restricting downstream dissemination of personal identifiers. In this way, the Minnesota Supreme Court could both protect the rights of accused people and address the injustices caused by disproportionate impact upon people of color. The best of both worlds is available.

Private data harvesters – those whose business it is to compile government data and sell it to private customers – dismiss as "vague supposition" the committee's concern about heightening disproportionate racial impact by unrestricted Internet dissemination of preconviction criminal court data. They oppose the recommendation in this report to restrict downstream dissemination of personal identifying information. They object to Bulk Data Alternative 1 as well, arguing that the court should provide to them—for unlimited global dissemination on the Internet—information such as litigants' and crime victims' Social Security Numbers, home addresses, and telephone numbers. While the data harvesters correctly state that public record data is central to society's "essential infrastructure," they also suggest that Bulk Data Alternatives 1 and 3 somehow attack that infrastructure by making public record data inaccessible.

This debate is about the correct use of new technologies, technologies that expand access to data in a way never imagined by the Founders, or even by policy makers a decade ago. This debate is not about any obligation by the Minnesota Supreme Court to help private data harvesters do their business in the most cost efficient and convenient manner possible. The Minnesota Supreme Court has no such duty. The Minnesota Supreme Court's duty is to protect the presumption of innocence and to ensure that no social group is stigmatized by the unrestricted dissemination of personal identifiers in preconviction matters.

THE COURT'S POLICY ABOUT DISSEMINATION OF ITS DATA SHOULD BE GUIDED BY ACCEPTED PRIVACY DESIGN PRINCIPLES

The impact of computers on individual privacy rights was the focus of a commission appointed in 1972 by then-Secretary of Health, Education, and Welfare, Elliott Richardson. The commission developed the "bill of rights for the computer age" called the Fair Information Principles (FIPs).[123] The FIPs were adopted by the Organization for Economic Cooperation and Development (OECD) to guide the development of and access to information systems. The FIPs are internationally

[123] U.S. Dept. of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems: *Records, Computers, and the Rights of Citizens* (July 1973); see http://www.epic.org/privacy/consumer/code_fair_info.html

accepted and acknowledged as a solid foundation upon which to build the sort of policy now being considered by the Minnesota Supreme Court.[124]

The following FIPS are particularly relevant to the bulk data decision faced by the Minnesota Supreme Court:

- **The *Data Quality Principle* requires agencies to verify the accuracy, completeness, and currency of their information.** Internet dissemination of inaccurate information would cause disastrous results. The court system in Minnesota is addressing acknowledged data quality problems with its longtime record-keeping system, TCIS. A new system, MNCIS, is being implemented on a county-by-county basis. It is assumed that the new system will increase accuracy, but the advisory committee has seen no proof that accuracy has begun to increase. The oldest problem and the problem most difficult to overcome with any data system is data entry error, casually referred to as "garbage in, garbage out." An examination of Internet-posted court data from Hennepin County, discussed earlier in this report, suggests that data entry inaccuracies are extensive in that system.

- **The *Purpose Specification, Collection Limitation* and *Use Limitation Principles* require agencies to specify in writing the purpose of their data system and limit use and dissemination to the stated purpose.** Once an agency has collected information, it is responsible for its appropriate downstream use and dissemination. Providing of bulk data to harvesters without any restrictions to its circulation runs afoul of these principles because it is difficult or impossible to control downstream compilation and use unless downstream distribution of these data is limited. Data gathered for legitimate court purposes may in a different context be used for destructive purposes. Consider use by a child searching court data on her parent, or students in a classroom checking out their teacher. Bulk Data Alternative 1 would allow an unsubstantiated accusation to follow an individual for life, forever tainting that individual's career and personal relationships.

Setting forth the argument made in opposition to unrestricted bulk distribution of court data, the National Criminal Justice Association in its *Justice Information Privacy Guideline* offers the following:

---

[124] *Justice Information Privacy Guideline: Developing, Drafting, and Assessing Privacy Policy For Justice Information Systems,* National Criminal Justice Association, September 2002, Chapter 3. (see http://www.ncja.org/pdf/privacyguideline.pdf)

"[Release of] large quantities of records at one time increases analysis and unintended use possibilities. Data analysis is not detrimental to personal privacy, per se. It can be used beneficially to show, for example, crime trends, treatment effectiveness, and "at-risk" groups, and to support justice planning and budgets. Analysis can have more personal consequences, however, depending upon who is using the information and for what purpose.

"For instance, the commercial sector can analyze court or corrections data to determine which heads of households have been incarcerated and use this data to market targeted services or products to the offenders' families, such as security systems, credit cards, and home equity loans. In another example, bulk data could be analyzed to isolate names of victims or family members and do targeted marketing on services or products. Picture a rape victim being inundated by junk mail for stress relievers, women's magazines, counseling, self-defense programs, athletic equipment, and even gun stores. Sound a bit unpalatable? Unfortunately, it is not far from reality.[125] Inaccuracies from unanticipated manipulation and analysis of bulk information are also problematic. Secondary users are not always mindful of the original purpose for which the information was collected and the "metadata" [126] that supports the information. Such analysis can result in inaccurate conclusions regarding the persons identified in the bulk data.

"Bulk data also feeds the development of "information profiles" that are being talked about in the context of e-commerce. Generally, the public is resisting the development of e-profiles on their living habits by commercial organizations. Bulk data available from the justice system can be used to supplement what was personal-choice information with criminal or related justice information.

"For example, it may be quite easy for your employer or insurance company to obtain your profile from an electronic information service showing that you shop at a certain discount store, purchase ice cream

[125] To avoid this type of use, some states have statutes prohibiting the use of criminal justice records for the solicitation of business. *See, e.g*., Colorado's Criminal Justice Records Act, Section 22-72-305.5.

[126] Simply stated, metadata is information that describes the pieces of information – or "information about information" (footnote in original).

> and bacon every week, have three kids, pay child support for two more, like action movies (especially the violent Rambo kind), smoke, vacation at the lake, bought a fishing boat, and were arrested for possession of marijuana 10 years ago. Do you sound like someone who might be a health or employment risk? Does this profile provide an accurate picture about you? Who decides what that picture means in terms of employability or insurability? Even further, commercial information services are used by law enforcement agencies for investigations.[127] The addition of justice information to e-profiles and their use by law enforcement make the discussion even more important in relation to individual rights and liberties.
>
> "Bulk data opponents argue that the majority of bulk data use is driven by profit, not responsible use of justice information. Companies can request one piece of information at a time, but the value added by bulk data is in receiving large quantities of information in a single transaction. The sheer speed and ease in which large quantities of information can be released, manipulated, and re-released compounds the inherent dangers in potentially improper secondary uses of justice information."[128]

Many or all of the destructive effects of bulk dissemination of court data can be avoided by requiring bulk data recipients to sign an agreement not to disseminate personal identifying information (name, date of birth, address, etc.) to downstream sources. Data harvesters would not be able to post personal identifiers on the Internet. E-profilers would be unable to use court data to prepare dossiers for targeted marketing purposes. Yet those seeking to learn about the criminal justice system – students, researchers, journalists – would have full access to court data.

Thus, restricting the downstream dissemination of personal identifying information in preconviction matters is the best way to both ensure openness and accountability of the courts, and to protect Constitutional rights of the accused. Language that would

---

[127] The FBI routinely consults on-line databases to obtain public source information regarding individuals, businesses, and organizations that are subjects of investigations. See, Statement of Louis J. Freeh, Director of the Federal Bureau of Investigation before the Senate Commission on Appropriations Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, March 24, 1999 (footnote in original).

[128] *Id*. At 54-55

accomplish this restriction is found in Bulk Data Alternative 3 set forth in Exhibit A at Rule 8, subd. 3.

THE DEPARTMENT OF REVENUE PROVIDES PROTECTIONS MORE EXTENSIVE THAN THOSE PROPOSED BY BULK DATA ALTERNATIVE 1

At least one other data-intensive state agency, the Department of Revenue, has taken a much more careful approach to data dissemination than Bulk Data Alternative 1. The Department of Revenue posts tax debtor names and debt amounts on a web site called DelinqNet.[129] But it takes a lot more than an unproven allegation for a person's name to appear on DelinqNet.

To be posted, the case must involve a severe matter (**more than 6 months delinquency and $5,000 or greater tax debt**); in contrast, those supporting Bulk Data Alternative 1 urge the Court to disseminate information about every adult matter on the court calendar, including the smallest embarrassing misdemeanor and petty misdemeanor. The Revenue Department requires a final determination be made by a neutral magistrate (**a lien or judgment must be recorded**); in contrast, those supporting Bulk Data Alternative 1 suggest just an accusation should be enough for the Minnesota Supreme Court to release data for dissemination. Finally, the Revenue Department gives the data subject 30 days to clear up any mistakes (**notification of data subject by certified mail 30 days prior to posting**); no similar pre-posting protection of criminal court data subjects is contemplated by those supporting Bulk Data Alternative 1.

Finally, note that the main difference between the constituencies affected by the Department of Revenue and the court system is the economic status of the data subjects. The majority urges broad Internet dissemination of sensitive, potentially damaging personal information affecting those accused of crimes, a population of people consisting predominantly of the poor.[130] Revenue Department data subjects are less likely to be poor: that is, they have at one time had an income for which they face tax liability. The Constitution and the presumption of innocence compels the Minnesota Supreme Court to be at least as diligent in protecting the rights of the poor as the Revenue Department is in protecting people with incomes.

---

[129] *See* http://www.taxes.state.mn.us/mce/delinqnet/requirements_for_posting.shtml

[130] Eighty to 90 percent of felony defendants, more than 90 percent of juvenile defendants and about half of misdemeanor defendants in Minnesota have so little income that they qualify for public defender appointment, according to State Public Defender John Stuart.

CONCLUSION

The advisory committee left unsolved the problems created by unreliable court data and the Constitutional mandate to protect those individuals accused of crimes but not yet convicted. The committee seems to have relinquished any responsibility for the use of information provided by the courts to bulk data harvesters. Determining the proper course of action is always a struggle in matters that require a balance between individual and public rights. The ethical standards embodied in the Fair Information Principles, which require that the Minnesota Supreme Court be certain of the quality of its data and that the court assume responsibility for the appropriate downstream use and dissemination of its data can and should provide guidance to the Court. The court system should not accomplish by proxy what it declines to do directly.

-- Robert Sykora
-- Van Brostrom
-- Donald A. Gemberling
-- Hon. Natalie Hudson
-- Jane F. Morrow
-- Teresa Nelson
-- Pamela McCabe
-- Hon. John R. Rodenberg
-- Lolita Ulloa (supports all aspects expect those parts based on the argument that court data are unreliable)
-- Gary A. Weissman

Exhibit L: Dissenting Statement on Internet Access to Judicial Records and Supporting Statement on Bulk Data Alternative 2

It has been a privilege to serve as a member of the advisory committee. It is difficult to imagine issues of greater importance in our democracy than those concerning the public's access to the records of its government. I have been honored to consider those issues in the company of such knowledgeable and experienced professionals. It is therefore with great reluctance, and only because of how critical I believe those issues to be, that I must respectfully disagree with the majority report's recommendations concerning Internet access to judicial records and Bulk Data Alternative 1.

The issues surrounding access are so important and complex that I believe more time and thought is necessary to ensure that we pay appropriate attention to the value of public access to judicial records, identify with precision those specific harms that are realistically posed by different forms of access to different types of judicial records, and then recommend precise rules to prevent those harms while facilitating robust public access to judicial records.

Alternatively, the Minnesota Supreme Court could try to correct the greatest shortcomings of the current report, especially as it applies to remote access, through three essential changes: (1) permit bulk access to complete judicial records in Rule 8, Subdivision 2(a) (or, at a minimum, all information about litigants/parties) by eliminating data element restrictions applicable to vital information such as Social Security Numbers, home addresses, and telephone numbers; (2) eliminate the restriction proposed in Rule 8, Subdivision 2(c) that would restrict courts from providing Internet access to searchable criminal docket information; and (3) require the close monitoring of, and regular reporting to the Court about, the way in which redaction and other administrative burdens imposed by the proposed restrictions work in practice to ensure that they do not result in more information than is specified being restricted, that they do not cause delay in making records public, and that they do not result in records or parts of records that should be made public under the proposed rules being withheld.

1. The Importance of Public Access

Public access to government records is critical to the operation of democratic self-government. The intrinsic relationship between self-determination and access has been recognized since the founding of the Republic. "A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or perhaps both," James Madison wrote almost two centuries ago.

"Knowledge will forever govern ignorance: And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives."[131] This commitment is reflected today in the federal Freedom of Information Act and similar laws adopted in every state.

Access to public records takes on special importance in the context of the judicial system, because it is through courts that law is applied most directly to individuals. Public access allows every citizen—whether directly or through commercial providers or other intermediaries, such as journalists—to monitor the activities of the courts, understand the operation of the law, be assured that the system is fair and just, be confident that the guilty are being identified and punished, and evaluate the cost-effectiveness and efficiency of our judicial system.

The value of access is not limited to the public's involvement in the judicial process, it also is an essential foundation of the press' ability to gather information and inform the public about other matters of public importance. Judicial records are critical to many of the stories that journalists write every day about public officials and the activities of the government. For example, the *Star-Tribune* built a database from bulk access to court records to demonstrate funding improprieties involving the Minnesota Partnership for Action Against Tobacco. The *St. Petersburg Times* searched judicial records to discover that a man running for city treasurer had not disclosed that he had filed for personal bankruptcy three times and corporate bankruptcy twice, and that the new director of a large arts organization that solicited donations had been charged with fraud in his home state. Tampa's News Channel 8 mapped the location of all drug arrests—information obtained from judicial records—to uncover a narcotics ring across the street from an elementary school. There are dozens of other examples involving court records. Each involves a published or broadcast public interest story that depended on electronic access—usually bulk access—to judicial records.[132]

In fact, a 2000 study by Elon University Professor Brooke Barnett found that journalists routinely use public records not merely to check facts or find specific information, but to actually generate the story in the first place. According to that study, 64 percent of all crime-related stories, 57 percent of all city or state stories, 56 percent of all investigative stories, and 47 percent of all political campaign stories rely on judicial and other public records. Access to public record databases is "a *necessity*

[131] Madison, Letter to W.T. Barry, Aug. 4, 1822, *reprinted in* 9 *The Writing of James Madison* 10 (Hunt ed. 1910).
[132] *See, e.g.*, Reporters Committee for Freedom of the Press, *Stories Using Electronic Court Records* (available at www.rcfp.org/courtaccess/examples.html).

for journalists to uncover wrongdoing and effectively cover crime, political stories and investigative pieces."[133]

Perhaps the least discussed, although most widely shared, benefit resulting from accessible judicial records is the use of those records as part of the critical infrastructure of our information economy. Reliable, accessible public records are the very foundation of consumer credit, consumer mobility, and a wide range of consumer benefits that we all enjoy. There is extensive economic research from the Federal Reserve Board and others that demonstrates the economic and personal value of accessible public records, but it does not require an economist to see that lenders, employers, and other service providers are far more likely to do business with someone, and to do so at lower cost, if they can rapidly and confidently access information about that individual.

The data elements necessary to determining whether a loan applicant has defaulted on past debts or a job applicant has a criminal record or a history of civil judgments reflecting on his or her character or honesty, require rapid access to data from around the country, with sufficient precision to identify and match individuals. This necessarily, inevitably requires access to account numbers, addresses, and Social Security Numbers. How else is one to distinguish among the more than 60,000 "John Smiths" in the United States, the more than three million people who change their names because of marriage or divorce each year,[134] or the 43 million Americans—17 percent of the U.S. population—who change addresses every year.[135]

Access to public records is particularly important for workers who are moving from one place to another in our highly mobile society, for the speed with which services are provided, and especially for economically disadvantaged Minnesotans. In short, accessible public records, and especially judicial records, facilitate consumer mobility, economic progress, and a democratization of opportunity. This is why the authors of the leading study of public records access concluded that such information constitutes a critical part of this nation's "essential infrastructure," the benefits of which are "so numerous and diverse that they impact virtually every facet of American life. . . ." The ready availability of public record data "facilitates a vibrant

---

[133] Barnett, *Use of Public Record Databases in Newspaper and Television Newsrooms*, 53 FED. COMM. L. J. 557 (2001) (emphasis added).

[134] National Center for Health Statistics, *National Vital Statistics Reports*, vol. 51, no. 8, May 19, 2003, at 1, table A.

[135] United States Postal Service Department of Public Affairs and Communications, *Latest Facts Update*, June 24, 2002.

economy, improves efficiency, reduces costs, creates jobs, and provides valuable products and services that people want."[136]

Judicial records are used to identify and locate missing family members, owners of lost or stolen property, witnesses in criminal and civil matters, debtors, tax evaders, and parents who are delinquent in child support payments. The Association for Children for Enforcement of Support reports that public record information provided through commercial vendors helped locate over 75 percent of the "deadbeat parents" they sought.[137] New York City's Child Support Enforcement Department used public record information supplied by ChoicePoint to recover $36 million over two years from thousands of non-custodial parents.[138]

Law enforcement relies on judicial and other public record information to prevent, detect, and solve crimes. In 1998 the FBI alone made more than 53,000 inquiries to commercial on-line databases to obtain a wide variety of "public source information." According to then-Director Louis Freeh, "Information from these inquiries assisted in the arrests of 393 fugitives wanted by the FBI, the identification of more than $37 million in seizable assets, the locating of 1,966 individuals wanted by law enforcement, and the locating of 3,209 witnesses wanted for questioning."[139]

---

[136] FRED H. CATE & RICHARD J. VARN, THE PUBLIC RECORD: INFORMATION PRIVACY AND ACCESS—A NEW FRAMEWORK FOR FINDING THE BALANCE (1999).

[137] Hearings before the Committee on Banking and Financial Services, U.S. House of Representatives, July 28, 1998, (statement of Robert Glass).

[138] Story is available on ChoicePoint website (http://www.choicepoint.com/news/success.html.).

[139] Hearings before the Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary and Related Agencies of the Comm. on Appropriations, U.S. Senate, March 24, 1999 (statement of Louis J. Freeh).

2. The Importance of a Legal Right of Access

It is precisely because of the political, economic, and societal importance of judicial records that the U.S. Supreme Court has found a constitutional right of access to the courts—the only branch of government to which the Court has applied such a right.[140] Public access is so essential that the Court has required that access be permitted to every phase of a trial, including voir dire, where privacy interests are arguably at their highest.[141] Access is required even over the objections of both the defendant and the prosecution.[142] Even when minor victims of sexual offenses were involved—when privacy rights are unmistakably at their apex—the Supreme Court unanimously struck down a Massachusetts ordinance that would have presumptively prohibited public access.[143] The Court has repeatedly extended the constitutional right of access to judicial records as well.[144]

This constitutional right of access to judicial proceedings and information merely restates the historical common law right of access.[145] Virtually all states have similarly recognized what the authors of the best-selling communications law casebook describe as "the long-standing practice of allowing inspection of court records by anyone wishing to do so."[146] This is certainly true in Minnesota, where the Minnesota Supreme Court has found that "[i]t is undisputed that a common law right to inspect and copy civil court records exists."[147]

I describe the common law and constitutional rights of access, not to suggest that they mandate access to all information in all court records under all circumstances, but rather to highlight the United States and Minnesota Supreme Courts' commitment to ensuring access to judicial records and the lengths to which both courts have gone to guarantee such access. The extraordinary degree of access that courts have sought to ensure where judicial records were involved reflects the critical role that access to such records plays in our democracy, economy, and society.

3. The Impact of Technology

---

[140] *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555 (1980).
[141] *Press-Enterprise Co. v. Superior Court*, 478 U.S. 1 (1986).
[142] *Richmond Newspapers*, 448 U.S. 555.
[143] *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596 (1982).
[144] *Press-Enterprise Co. v. Superior Court*, 464 U.S. 501 (1984); *Press-Enterprise*, 478 U.S. 1.
[145] *Nixon v. Warner Communications, Inc.*, 435 U.S. 589 (1978).
[146] MARC A. FRANKLIN, ET AL., MASS MEDIA LAW 762 (6th ed. 2000).
[147] *Minneapolis Star & Tribune v. Schumacher*, 392 N.W.2d 197, 202 (Minn. 1986).

The question the Minnesota Supreme Court asked our committee to address is whether technology affects the degree to which or the way in which our judicial system provides the public with the access it needs and is constitutionally entitled to have. This is a very difficult question, as the Minnesota Supreme Court wisely recognized, and requires balancing the demonstrated benefits of access with the potential for harms that access facilitates.

a. The Importance of Balance

In attempting to answer the Minnesota Supreme Court's question, the majority of the committee appears to have placed heavy emphasis on only one side of the equation—the potential for harm. The introduction to the majority report focuses almost exclusively on the concerns related to Internet access. Only in a few footnotes is there reference to testimony regarding the benefits of access and the purposes it serves.

The emphasis on harm is most evident in the majority's consideration of Internet to Minnesota court records. The majority begins its discussion by noting that "[a]ccess to court records is becoming easier and much broader now that an electronic format replaces or augments paper. The Internet's capacity to consolidate information into easily searchable databases means that the trip to the courthouse is a virtual journey accomplished with the click of a computer mouse."[148]

This is great news: the Internet and electronic access through commercial intermediaries are making widespread, affordable, convenient public access to judicial records practical for the first time in our history. They are helping to turn the theoretical promise of access into a practical reality for all Minnesotans. But rather than celebrate this development, or even reference its positive impact on the constitutional promise of open records, the majority instead laments the fact that "[t]hese changes have eroded the practical obscurity that individuals identified in court records once enjoyed," and then outlines a parade of "competing and often conflicting interests including, but not limited to, protection against unsubstantiated allegations, identity theft protection, accuracy, public safety, accountability of courts and government agencies, victim protection and efficiency."[149] Had the majority focused as much on the many demonstrated benefits of public access as it did on the possibility of potential harms, the subsequent analysis might have been more balanced and thoughtful.

[148] Report, at 4.
[149] *Id.* at 4-5 (citation omitted).

b. The Importance of Supporting Data

Exacerbating this tendency towards a one-sided presentation of the access issue is the fact that the majority provides supposition and anecdote in lieu of actual data about the prevalence and impact of the asserted harms and the relationship between those harms and access to judicial records. In fact, the majority cites no evidence that electronic access to judicial records has ever resulted in a measurable harm. I do not for a moment suggest that judicial records could not be used to cause harm, but before severely restricting Internet and bulk access, I would have liked to have more than vague supposition about the existence and magnitude of those harms.

c. The Importance of Relevant Data

It is even more troubling that the majority's assertions about those harms ignore relevant and reliable information about their nature and cause. For example, the majority repeatedly cites to identity theft as a concern posed by access to judicial records, but this conflicts with the Federal Trade Commission's comprehensive study of identity theft, published in September 2003. That report, based on more than 4,000 interviews, found that public records of all forms played such an insignificant role in causing identity theft as to be immeasurable. In fact, that study found that, of the one-quarter of identity theft cases in which the victim knew the identity the perpetrator, 35 percent involved a "family member or relative" and another 18 percent involved a friend or neighbor.[150] The majority's discussion of identity theft would lead one to think that electronic access to judicial records was a major contributor to this crime, when the FTC's data suggest it is not.

The majority also fails to note the critical role that access to public records plays in *preventing* identity theft. Bulk access is vital to employment screening, identity verification, and other services that businesses use to ensure that the person seeking credit, borrowing money, or applying for a benefit is who he or she claims to be. The evidence suggests that reducing access to judicial records is more likely to increase than reduce identity theft.

This is also true with regard to the problems faced by persons of color who, as the report notes, may be arrested for certain crimes at such a disproportionate rate as to suggest discrimination by law enforcement officials. Public access to this information does not cause the problem; rather, as the majority report concedes, public and press access is essential to exposing and solving it.

---

[150] Federal Trade Commission, *Identity Theft Survey Report* at 28-29 (Sept. 2003).

4. The Majority's Recommendations Concerning Internet Access and Bulk Data Alternative 1

In my view, neither the majority report nor the testimony and documents with which the committee was presented establish any meaningful connection between electronic access to public records and harm, much less a realistic probability of sufficiently serious harm to warrant compromising the access that the public has long enjoyed and to which it is entitled.

Even, however, if for the sake of argument alone, we assume that a connection between access to judicial records and the harms identified by the majority could be established, the majority's recommendations are so blunt and broad that they are unlikely to afford the public any significant protection, while undermining the benefits of accessible judicial records. There are many examples, but I will provide just five.

a. Shifting the Burden

Perhaps because of the majority's focus on possible harms that might result from access to judicial records, to the exclusion of recognizing the benefits of access, the majority and the supporters of Bulk Data Alternative 1structure their recommendations concerning Internet and bulk access in the most restrictive manner possible. Rather than follow the traditional approach used in federal law and virtually every state of providing for public access to all public records, except for those specifically determined to pose a specific risk of harm, the majority and the supporters of Bulk Data Alternative 1 take the virtually unprecedented approach of allowing Internet and bulk access only to a list of documents; everything not listed is excluded: "[a]ll other electronic case records that are accessible to the public under Rule 4 shall not be made remotely accessible. . . ."[151]

This turns the constitutional presumption of openness on its head. In *Globe Newspapers Co.*, the United States Supreme Court refused to allow the Massachusetts legislature to presumptively close courtrooms during the testimony of minor victims of sexual offenses. Despite the magnitude of the potential risk and the fact that the state law was limited exclusively to protecting children, the Court found that in every instance in which a judge determined to close a courtroom, the judge must first specifically determine that the "denial [of access] is necessitated by a compelling governmental interest, and is narrowly tailored to serve that interest."[152]

[151] Report, at 56 (proposed Rule 8, subd. 2(b)).
[152] 457 U.S. at 606.

The people of Minnesota deserve no less protection, especially where, as here, the majority has provided no evidence as to the realistic potential for harm if Internet or bulk access is provided. This is what the law requires: in Minnesota court records are presumptively open and a person seeking to block access must assert "strong countervailing reasons."[153] Rather than provide a list of what is permitted, and exclude all else from electronic access, the majority and those supporting Bulk Data Alternative 1 should have sought to identify those data elements that could be demonstrated to pose a specific risk of harm to the public, and then restricted electronic access only to those.

It is no answer to say that access is still available at the courthouse. First, it isn't accurate; the majority recommends prohibiting access to some information altogether. Second, and more importantly, it isn't adequate. U.S. courts and U.S. law has long required that access must be as robust as is feasible within existing financial and technological resources. Minimum access is not enough, if broader access could reasonably be provided. Chief Justice John Marshall, sitting as a specially designated trial judge, moved the trial of Aaron Burr from the courthouse to a larger hall so that more people could be accommodated. Almost 200 years later, Congress amended the Freedom of Information Act to specify that records must be provided in the medium and format requested unless it was impractical to do so. This highlights a third fallacy of the "some access" argument: forms of access are not interchangeable, but the majority treats them as if they were. Courthouse access is no substitute for access from across the state, and access to individual paper records is no substitute for electronic access to the entire database.

Finally, the majority's recommendations on Internet access combined with Bulk Data Alternative 1 restrict access to key data elements to the courthouse alone. This ignores U.S. and Minnesota Supreme law and principles requiring the proponents of any new restriction of access to demonstrate why it is warranted, irrespective of whether other forms of access are available.

b. Confusing the Interests of Litigants, Jurors, Witnesses, and Victims

The majority's recommendations on Internet access and Bulk Data Alternative 1 repeatedly lump together the interests of "litigants, jurors, witnesses and victims," despite the fact that the interests of these parties have long been recognized to vary widely. Litigants who choose to go to court to seek the judiciary's assistance in resolving a civil dispute clearly have different—and weaker—interests in secrecy than do the victims of crime. Similarly, the public's interest in information about these

[153] *Minneapolis Star & Tribune v. Schumacher*, 392 N.W.2d at 206.

parties differs greatly. While the public clearly has a legitimate interest in knowing that a jury is fair, impartial, and representative, knowing the Social Security Numbers of individual jurors is not necessarily relevant to that task. On the other hand, knowing the Social Security Numbers—the only form of uniform identifier used in the United States—of a person who is disposing of assets or seeking to avoid debts is of the greatest importance.

The majority report on Internet access and Bulk Data Alternative 1 ignore these distinctions entirely and inexplicably makes no differentiation whatever among "litigants, jurors, witnesses and victims" or "parties or their family members, jurors, witnesses, or victims." This is a serious flaw that is easily remedied by addressing the interests of litigants or parties separately from those of jurors, witnesses, and victims.

c. Confusing Courthouse Access with Internet and Bulk Access

Despite having asserted a variety of harms alleged to result from traditional access to judicial records, the majority recommends few new restrictions on courthouse access, while recommending substantial new limits on Internet access and, in Bulk Data Alternative 1, bulk access. Yet neither the majority nor the supporters of Bulk Data Alternative 1 explain why these categories of access should be treated differently.

Presumably—and the public can only presume here because the majority and those supporting Bulk Data Alternative 1 are silent—those supporting the majority position on Internet access and Bulk Data Alternative 1 believe that there are fewer obstacles to a perpetrator of identity theft or other fraud obtaining information remotely than at the courthouse. For example, a criminal is likely to desire anonymity, and the committee may be assuming that anonymity is easier to obtain through remote access. Such beliefs if held are not based on reality. Access via the courthouse historically is anonymous: an individual does not have to provide his or her name to exercise a constitutional right. Moreover, the committee's recommendations would allow for electronic access at a courthouse. If this access is provided through public kiosks, like public access to the Internet is provided at Minnesota public libraries, there will be no occasion for identification.

Ironically, Internet and bulk access, by contrast, do tend to leave the electronic version of a "paper trail" that would allow investigators, months or even years later, to determine who obtained access to a specific record. If payment is required for printing or downloading or to access a commercial service, some form of identification—for payment—is inevitable. No evidence has been presented to the committee that suggested that Internet or bulk access was less reliable or more risky than courthouse access—only that it was less expensive, more convenient, and more accessible for people who live in remote communities or have limited mobility. The available

evidence argues for more, not less, electronic access, if we are interested in serving the people of Minnesota.

d. Confusing Internet and Bulk Access

Nowhere is the lack of precision in the advisory committee's recommendations clearer than with its confusion of bulk access with Internet access. Those supporting Bulk Data Alternative 1 lump bulk and Internet access together, thereby ignoring significant differences between the two. Bulk access is most often obtained by commercial subscription services, such as Westlaw and Lexis, who make the data available to identified subscribers, including law firms, private investors, credit bureaus, and law enforcement agencies. Commercial intermediaries buy judicial records in bulk and then add value by combining information from multiple sources, adding useful finding and interpretive aids, and making standardized information available conveniently, reliably, and at low cost. These commercial information providers both enhance access, with all of its benefits—constitutional and otherwise—and greatly reduce the burden on court clerks by filling many requests for records that would otherwise consume court resources.

As a result, many Minnesota attorneys and businesses use services provided by Westlaw, Lexis, and other commercial providers for convenient, desktop access to court records, rather than apply to courts themselves for those records. Similarly, journalists increasingly rely on commercial intermediaries. And the economic benefits that all Americans share from open court records depend entirely on commercial providers: Lenders, retailers, employers, professional associations, child care facilities, and others who need to verify information about past criminal activities turn not to court clerks, but to commercial intermediaries for this information.

Ironically, even the government looks to commercial providers for public record data. Courts across the country use Westlaw, Lexis, and other commercial providers, as do law enforcement agencies. According to former FBI Director Louis Freeh, access to commercial providers of public record information "allows FBI investigative personnel to perform searches from computer workstations and eliminates the need to perform more time consuming manual searches of federal, state, and local records systems, libraries, and other information sources. Information obtained is used to support all categories of FBI investigations, from terrorism to violent crimes, and from health care fraud to organized crime."[154]

[154] Hearings before the Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary and Related Agencies of the Comm. on Appropriations, U.S. Senate, March 24, 1999 (statement of Louis J. Freeh).

Bulk buyers also provide significant financial revenue for public records custodians, including courts, as well as other services, such as returning to the custodian records that have been updated, formatted, or otherwise corrected. Anonymous access is rare: you must have an account and password to log-on. Even those entities that do make such data available on-line, charge a fee for doing so and therefore typically require identification. Thus, the access provided by bulk buyers is typically more secure, not less, than that provided directly by courts. Direct Internet and courthouse access provide none of these benefits or protections.

It is nonsensical to lump bulk access together with Internet access, or to apply the identical rules to both, without discussion of the significant differences between the two. Moreover, it is inappropriate to lump all bulk requesters together. If the advisory committee's concern is ensuring accountability, then bulk access by subscription services, which require subscriber identification, operate subject to contracts with both public information providers and subscribers, and have a long history of responsible service to both courts and subscribers should not be blindly grouped together with one-time requesters or nonsubscription services.

e. The Administrative Burden of Redaction and Other Requirements

The rules changes on Internet access proposed by the majority and Bulk Data Alternative 1 pose serious questions as to how they will work in practice and the burden they will create on court clerks and other judicial officials. Certain data, such as street addresses and telephone numbers, never be disclosed via Internet or in bulk. How is this to be accomplished? These data elements presumably will still be required on court filings. The information will be available at the courthouse, possibly even through electronic systems. How are these data to "disappear" when the document is accessed via Internet?

In the advisory committee's discussions, it has been suggested that this will be accomplished primarily by placing the responsibility on attorneys to segregate such information. The proposed rule, however, places the burden far more broadly and, in any event, many judicial records are not prepared by attorneys, and it is inappropriate in any event to place the burden on them of ensuring that redaction rules are followed. This is not a problem that technology is likely to solve affordably or consistently. The likely results are increased burdens for already over-worked judicial staff, delays in making records accessible to the public, or most seriously, the wholesale withholding of documents containing the specified data elements.

A similar concern is raised by the majority's recommendation that Internet access to "preconviction criminal records" on the Internet be conditioned on those

records being "not searchable by defendant name using automated tools."[155] In part, this rule would place restrictions on criminal dockets available via Internet by ensuring that the docket is not searchable by defendant name. The proposed restriction is unprecedented in any state I have examined. It also seems undesirable, which may explain why no other state has taken this step, to restrict electronic access to the docket itself—not the parties' filings or supporting papers, but the actual barebones record of what our courts are up to. Again, no state has placed limitations on Internet access to docket information and Minnesota should not be the first.

5. Conclusion

The committee's many meetings and extensive research provide a solid foundation for recommending to the Minnesota Supreme Court thoughtful rules for ensuring that Minnesota residents continue to have open access—and realize the potential of the Internet and commercial intermediaries to provide even wider, more convenient, and less costly access—to the records of their court system, while protecting against specific, identified harms realistically posed by expanded accessibility.

Regrettably, the majority recommendation regarding Internet access and Bulk Data Alternative 1 do not deliver on that potential. Instead, they minimizes the historical, constitutional, and practical arguments in favor of access, and focuses instead on broad, unsupported assertions about the harms that might possibly result from access. Instead of tight analysis, these recommendations concerning Internet and bulk access are based on anecdote and innuendo. As a result, those recommendations are too broad and blunt to provide the precision that any effort to restrict public access to judicial records requires.

In particular, these recommendations rest on an unstated, and certainly untested, assumption that Internet and bulk access present greater risks to the public than access (including electronic access) at the courthouse. The inexplicable refusal of the supporters of Bulk Data Alternative 1 to distinguish between bulk and Internet access lead it to make recommendations that not merely fail to serve the public's interest, but actively disserve it. Westlaw, Lexis, and similar commercial services provide widespread access in every corner of Minnesota to critical, enhanced information. This reduces the burden on court clerks and other public records custodians, generates significant revenue for the state, and provides a valuable resource for state government agencies as well as attorneys, businesses, and the public. Yet, without properly noting these benefits or providing sufficient

[155] Report, at 56 (Proposed Rule 8, subd. 2(c)).

explanation, the supporters of Bulk Data Alternative 1 recommend lumping this service together with Internet access and subjecting both to new stringent limits.

What is needed is further study to document the importance of public access to judicial records, identify with precision those specific harms that are realistically posed by different forms of access to different types of judicial records, and then recommend precise rules to prevent those harms while facilitating robust public access to judicial records.

Alternatively, the Minnesota Supreme Court could try to correct the greatest shortcomings of the current report, especially as it applies to remote access. At a minimum, I believe this would require three essential changes:

1. **Permit bulk access to complete judicial records in Rule 8, Subdivision 2(a).** The critical uses of court records by a wide range of government and business clients include: preventing identity theft, helping locate missing children, assisting in the enforcement of child support obligations, helping law enforcement locate witnesses to crimes and finding missing pension beneficiaries. These uses depend on gaining access to the complete record, including key personal identifiers as Social Security Numbers, home addresses, and telephone numbers. The restrictions in Rule 8, Subdivision 2(b) are overexpansive and restrict key personal identifiers such as home address and phone numbers that have traditionally (except in very limited circumstances) been available to the public. At a minimum, bulk access should include Social Security Number, home address, and telephone number information, at least for litigants and parties.

2. **Eliminate the restriction proposed in Rule 8, Subdivision 2(c), that would restrict courts from providing Internet access to searchable criminal dockets.** Internet access to criminal and civil dockets should be unimpeded.

3. **Require the close monitoring of, and regular reporting to the Minnesota Supreme Court about, the way in which redaction and other administrative burdens imposed by the proposed restrictions work in practice** to ensure that they do not result in more information than is specified being restricted, that they do not cause delay in making records public, and that they do not result in records or parts of records that should be made public under the proposed rules being withheld.

(continued next page)

While I believe it would be better for the Minnesota Supreme Court to grant the committee more time to develop rules based on evidence and reflecting the constitutional preference for openness, I believe that these three changes are essential to if we are to comply with what the Constitution requires and the people of Minnesota deserve.

Donna Bergsgaard

Joined by:

Acxiom Corporation
ChoicePoint Inc.
Coalition for Sensible Public Records Access
Consumer Data Industry Association
Equifax
Experian
First American Corporation
LexisNexis
TransUnion
West, a Thomson business

Exhibit M: Minority Report on Searchability of Preconviction Criminal Records by Defendant Name and Public Access to Race Census Data

Introduction

This submission addresses two important issues on which the advisory committee was closely divided:

> 1. Whether preconviction criminal records should be searchable by defendant name when posted by the courts on the Internet.
>
> 2. Whether race and ethnicity census data collected by the courts should be publicly accessible.

With respect to the first of these issues, the committee's final report recommends that preconviction criminal records, even though they are fully accessible to the public, should be posted on the Internet only in a manner that does not allow them to be electronically searched by use of the defendant's name. *See* proposed Rule 8, subd. 2(c). As for the second issue, the Report suggests that there be no general public access to race and ethnicity information, even though the court system has been collecting this information from criminal defendants for nearly two years, during which time it has been fully available to the public. *See* proposed Rule 4, subd. 1(e).

As discussed below, these recommendations are the product of good intentions but demonstrably flawed factual premises. They would accomplish virtually nothing in terms of what their proponents describe as the reasons for adopting them, while seriously interfering with a number of important values–including some that the Rules of Public Access are designed to foster. The recommendations should therefore be rejected or modified by the Minnesota Supreme Court.

1. Remote Searchability of Preconviction Records by Defendant Name.

Proposed Rule 8, subd. 2(c) states that "[a]ny preconviction criminal records posted on the Internet shall be made available only by using technology which, to the extent feasible, ensures that [the] records are not searchable by defendant name using automated tools." If adopted, this provision would cause preconviction criminal records to be treated differently than all other court records that the proposed Rules authorize remote (Internet) access to. It would severely inhibit the ability of citizens, attorneys, parties, and others to effectively use what is one of the most frequently employed databases maintained by the court system.

Proponents of the recommendation principally argue that Rule 8, subd. 2(c) is necessary to minimize the "imprimatur" that might otherwise be perceived by visitors to a court Website with respect to preconviction data–such visitors would somehow conclude that a criminal defendant was guilty even though not yet convicted, since the information appeared on the official court site. *See* Final Report, 4, 9, 15.[156] This view is coupled with a number of other objections, which focus on the concern that "making preconviction court records available to anyone at any time and in virtual perpetuity over the Internet will have a permanent, disproportionate impact on the housing and employment of persons of color, especially young men of color." Final Report, 14.

The issue of whether preconviction criminal records should be remotely accessible in searchable form was frequently addressed during the advisory committee's deliberations. In the end, the position described in proposed Rule 8, subd. 2(c) prevailed by a vote of 9 to 7—a bare majority of the committee members present on the day the vote was taken, and not a majority of the entire committee. *See* Report, 19.

This minority report asks the Minnesota Supreme Court to reject the recommendation. There are a number of readily evident defects in the arguments that the proponents have offered to support the proposed Rule.

First, at a pragmatic level, it is clear that the recommended Rule will accomplish nothing in terms of limiting the availability of searchable preconviction criminal records on the Internet. That is because a large number of other entities–both private and public–independent of the court system have for some time made, and continue to make, such records available on their Web sites. All of the criminal records at issue here are publicly accessible at the courthouse. This would not change under the advisory committee's recommendations. As its Final Report (at 10) acknowledges, if "the underlying information is public on paper, the information likely will be available from private-sector data brokers." It is available through public agencies as well.[157]

---

[156]References are to the Draft Final Report, since the Final Report was not completed at the time this submission was prepared. Thus, page numbers may be slightly different in the Final Report.

[157]See, for example, the Hennepin County Attorney's Web site (www.hennepinattorney.org), which provides considerable preconviction information about criminal matters, and which is in part expressly designed to help citizens actively participate in and follow judicial proceedings. Such sites are of course not governed by court access rules.

Thus, the specific consequences that the proponents of proposed Rule 8, subd.2(c) most zealously expressed concern about–the purported impact on housing and employment for persons of color—will simply not be ameliorated by the proposed Rule. The preconviction information will be widely available in a searchable form on the Internet regardless of what the Minnesota Supreme Court does. As the proponents of the proposed Rule effectively conceded during the committee's deliberations, its principal value would therefore be, at most, symbolic. It would have little or no practical benefit.

In contrast however, there would unquestionably be specific adverse consequences flowing from adoption of the proposed Rule. Prominent among them would be the impact on court system resources. One of the singular benefits offered by Internet access to court records is the potential for substantial efficiencies with respect to court staff time. There can be little doubt that when citizens, attorneys, and others using the court system are able to acquire routine information by visiting a court Web site, the number of phone calls and physical visits to court administration will be significantly reduced. Queries about criminal matters probably constitute one of the largest of all categories of requests for information fielded by district court staff. Thus preventing searches by defendant name will likely eliminate much of the benefit that Internet access to court records would otherwise provide, because efforts to locate the particular case or party in which a person is interested will often be slow and cumbersome given the volume of criminal records. It will frequently seem more convenient to simply make a phone call to the court administrator's office.

The advisory committee specifically considered this issue in the context of Hennepin County, which for approximately the past 10 years has operated a subscriber service allowing dial-up access (for a fee) to court records, including preconviction criminal records. Hennepin County district court officials were asked by the committee to estimate the impact of eliminating remote searchability of preconviction records, as suggested in proposed Rule 8, subd. 2(c). They responded that it would almost certainly affect their operations, surmising that at least two additional full-time employees could be required to handle the increased calls and counter visits. While these officials conceded that it was difficult to provide exact estimates, they left no doubt that there would be a definite consequence in terms of staff time and resources caused by proposed Rule 8, subd.(2)(c). If that potential impact is considered collectively with respect to all of the district courts in the state, the financial ramifications could be substantial.

There will be other costs for the court system that result as well. For example, the advisory committee's report acknowledges that posting only "non-searchable" preconviction records on the Internet affords no permanent solution to the alleged harms that searchability might cause, because it may be obviated by "technological

advances" that will allow the records to be searched regardless. *Id.* at 18. The report suggests that though this may be offset by "advances and vigilance" it "is anticipated that this will be a constant struggle." *Id.* In practical terms however, this "constant struggle" translates into potentially significant ongoing costs for the court system, and in the end will probably be futile anyway.

If incurring such expenses was likely to produce some sort of tangible benefit, then of course they might be justified. But as noted above, fully searchable preconviction criminal information is and will continue to be readily available on the Internet regardless of whether the court system supports it. Given the many other demands on the court system's resources, this minority report submits that the funds which would be expended on attempting to adequately administer proposed Rule 8, subd. 2(c) could be far better directed to other priorities–where some real advantages might accrue.

While it may be questioned whether anyone will in fact benefit from proposed Rule 8, subd. 2(c), there are many individuals and entities (in addition to the court system itself) that will be concretely and negatively affected by the anti-searchability provision found in the Rule. Though these parties are not always as visible or easily counted as those whom the proposed Rule is supposed to aid, they should nonetheless be considered. They include parties to criminal actions, witnesses, victims and their families, attorneys and other officers of the court, journalists, public employees (among them law enforcement officials) not part of the court system, neighborhood groups, various kinds of advocates, and court-watchers. All would benefit greatly from being able to efficiently monitor, via the Internet, the court system's treatment of criminal defendants during the preconviction phase of the proceedings.

However, banning the capacity to remotely search criminal court records by means of a defendant's name will significantly impede the ability of all these individuals and many others to effectively obtain the information that they are seeking from the court system. Not only will many of them, as discussed above, then burden employees of the court administrator's office by making phone calls or visits, but the additional time these persons must collectively invest in trying to obtain information will certainly be very considerable, and should also be taken into account in assessing the cost and impact of the proposed Rule. In short, the Rule will penalize the many potential beneficiaries of searchable on-line access to preconviction criminal data, without any corresponding benefit to defendants.

In addition to the advantages of time savings, convenience, and efficiency that would be realized, searchable remote access would more broadly promote accountability and accuracy with respect to the criminal court system--a value often identified by the Minnesota Supreme Court as one of the reasons warranting public

access in the first place–because of the expanded number of individuals and entities who could conveniently obtain access to criminal records by means of the Internet.

The value of such accountability can be demonstrated in many ways. For example, there are a significant number of criminal dispositions–typically achieved by means of a plea negotiation–that permit defendants to avoid a conviction even though they very well may be essentially guilty of what they were charged with. As the advisory committee's report notes, a continuance for dismissal, a diversion, a retention of unadjudicated offenses under MINN. STAT § 609.04 (2003), or a stay of adjudication may all result in no recorded conviction. *See* Report, 19-20. As a result, *none* of the records relating to such prosecutions would *ever* appear in searchable criminal records available on a court's Web site. Yet the community at large, as well as victims of criminal behavior, have a distinct interest in being able to readily monitor such proceedings and the resulting dispositions.

In addition, criminal records posted by the courts on their own Web sites are likely to be more accurate and up-to-date, as compared to those maintained by private data brokers. But if use of the court sites is inefficient, the data having more integrity will receive less attention. In addition, incorrect and outdated information about criminal proceedings that does exist in court records may go unremedied, because those most likely to notice–including criminal defendants themselves–will not have ready access to the records, and the errors will be perpetuated through private Web sites that they would rarely see.

Moreover, there is reason to believe that concerns about the potential adverse impact of searchable Internet access to preconviction criminal data have been exaggerated. It is worth noting, for instance, that while many state and federal courts have recently moved to make criminal records accessible via the Internet, none has imposed the cumbersome condition found in proposed Rule 8, subd. 2(c). Yet if it were in fact plausible that the sort of harm claimed by proponents of the proposed Rule would occur simply because preconviction criminal court records are searchable on court Web sites, it seems unlikely that no other jurisdiction would have acknowledged it. Furthermore, as noted above, Hennepin County has permitted dial-up access to criminal records for approximately 10 years, which includes searchable preconviction data. However, not a single demonstrated case of harm resulting from this access was presented to the Advisory Committee. Indeed, despite the fact that many commercial Web sites have long provided widespread access to preconviction data, no specific empirical evidence of harm attributable to such access was identified.

In other words, the case for proposed Rule 8, subd. 2(c) rests almost entirely on unsubstantiated speculation. [158]

This minority report contends that when the foregoing considerations are assessed, it is clear that many more benefits will accrue from allowing remote, searchable access to preconviction criminal court records as compared to what will happen if proposed Rule 8, subd. 2(c) is adopted. Neither alternative is perfect. However, since one must be chosen, the option that provides the more demonstrable and distinct advantages should be preferred.

Furthermore, the Minnesota Supreme Court has two relatively simple options by which to mitigate the claimed harm that would be caused by remotely searchable preconviction criminal records, while retaining most of the benefits. The first of these would be to require an explicit disclaimer that would appear whenever a court's criminal records are accessed on line, informing the Web site visitor that until a conviction is entered, defendants are presumed to be innocent of all charges, and that the state has the burden of demonstrating guilt beyond a reasonable doubt. Additional information could be provided as well, cautioning the visitor about misuse of such information. Indeed, such a notice would not only offset the purported "imprimatur" that supporters of proposed Rule 8, subd. 2(c) identify, but it could well be effective in counteracting the possible effects of commercial Web sites supplying preconviction criminal data, which typically do not contain any such notice. Thus access to preconviction criminal records through a court Web site in this fashion would, on a net basis, be likely to have positive effects rather than negative ones.

The Minnesota Supreme Court could also choose an intermediate option in terms of searchability, which would be based on the distinction between search engines external to a particular Web site (such as Google) and those available only once a particular Web site is reached. Selecting the latter would reduce the purported harms caused by casual Internet "surfing," something that the proponents of proposed Rule 8, subd. 2(c) have most focused on. Those who take the trouble to locate and visit a specific court Web site might be more likely to have a legitimate reason for doing so. In any event, both of these options–Web site disclaimers and limited, site-specific search engines–are preferable to Rule 8, subd. 2(c) as currently drafted.

---

[158] It can be observed that similarly dramatic and speculative claims were made to the Minnesota Supreme Court prior to its recent adoption of presumptive public access to child protection proceedings. Yet despite a lengthy experimental period allowing such access in several pilot counties, and then adoption of the public access rule on a statewide basis effective July 1, 2002, there has been no factual demonstration that the many dire predictions made by opponents of CHIPS access were warranted.

2. Public Access to Race and Ethnicity Census Data Collected by the Courts

The advisory committee also recommends that a new Rule 4, subd. 1(e) be adopted that would almost entirely prohibit public access to race and ethnicity census data collected by the court system. The Rule would create an exception to the normal presumption that governs court records, restricting access to the "contents of completed race census forms obtained from participants in criminal, traffic, juvenile and other matters," subject only to a few narrow exceptions. Again, this suggestion was adopted on a closely divided vote—indeed, by a one-vote margin. *See* Final Report, 29. The minority report takes the position that the Committee's recommendation conflicts with the very purposes for which the race census data are being collected in the first place, namely, to monitor the judiciary and provide some assurance that allegations of race bias in the court system are being properly addressed.

It can hardly be contested that claims of racial bias in the court system have been among the most difficult issues confronted by the judiciary in recent years. As the advisory committee's Final Report notes, the collection of race census data was recommended as a means of promoting racial fairness. *Id.* at 28-29. However, preventing public access to these data would threaten to markedly diminish the credibility of any claim by the court system that it is making headway with respect to the racial bias issue. That is because the proposed Rule would plainly inhibit independent, outside parties that might attempt to evaluate the treatment of racial and ethnic minorities in the judicial process. If the very entity against which the allegations have been made—the court system—is the only one that has full and convenient access to individual race and ethnicity data, then its capacity to credibly contend that progress is occurring by reference to that data will inevitably be suspect.

The two exceptions described in proposed Rule 4, subd. 1(e) authorizing some outside access are of little or no value in facilitating independent scrutiny using the race census data. In the first place, both accord a great deal of discretion to the court administration in terms of whether access is even permitted. History demonstrates that this constitutes a decidedly inconsistent and unreliable method of fostering accountability. Furthermore, both exceptions impose significant limitations on disclosure "to any third party." This considerably reduces the independent usability of such data. Moreover, both alternatives would effectively require the court administrator to obtain the identity of the requester in order to properly determine if an exception applies. Yet it is well understood that there are many instances where a person seeking to scrutinize government records would prefer to remain unidentified.

For this reason, the statute governing access to Minnesota's administrative branch records—the Minnesota Government Data Practices Act, Minn. Stat. ch. 13—contains an express provision barring public officials from demanding the identity of a requester of records as a condition of permitting access. *See* Minn. Stat. §13.05, subd. 12. In short, proposed Rule 4, subd. 1(e) will frustrate the very accountability that collection of race and ethnicity census data is designed to promote.

As the advisory committee report notes, a principal reason identified by the proponents of preventing public access to such data is based on the concern that disclosure would deter parties from completing the forms (which is voluntary). However, as with many of the concerns relating to remote searchability of preconviction criminal records, this is entirely speculative, and is in fact contradicted by experience. The race and ethnicity census forms have been in use for approximately a year and a half, according to information submitted to the committee. During that time, there has been no restriction on public access to the forms. Yet there is not the slightest empirically based indication that public access to the data they contain has in any way deterred participation. The committee was told that a very high percentage of those asked to complete the form have done so, without qualification. Furthermore, there was no evidence whatsoever presented suggesting that particular individuals who completed the forms have experienced any harm, or even that there have been concerns expressed by those parties.

Whether the judicial system does have a problem with racial bias and unfairness remains a question to be debated. However, if that question is to be credibly answered, effective public access to one of the main compilations of data by which the issue can be rationally assessed is essential. Thus this minority report also asks that the Minnesota Supreme Court reject proposed Rule 4, subd. 1(e), and instead continue to allow public access to the race and ethnicity census data.

-- Mark R. Anfinson
-- Donna Bergsgaard
-- Paul R. Hannah
-- Gene Merriam

Exhibit N: Special Fact Finding Subcommittee Report to Advisory Committee

April 30, 2004

The Fact Finding Subcommittee was directed to compile additional information on the potential impact of the competing Internet access and bulk distribution policies. The subcommittee examined the current majority proposal that limits automated searches of calendars and registers of actions, and precludes Internet posting of name indexes. The subcommittee asked what is the potential impact on the MNCIS project timeline and resources? It also asked what is the potential impact on current fourth judicial district electronic access customers? Related policy issues and information are also included in this report as they were part of the subcommittee's discussion and offer valuable insight for the full advisory committee.

MNCIS

Information presented by Bob Hanson, Supreme Court IT Director:

Modify the current viewing tool (referred to as MNCIS Public Access or "MPA") for presentation to the Internet

Option 1. Use case status to distinguish pre- and post-adjudication

a. Requires separating the current six User Case Statuses into pre- or post-adjudication categories (advisory committee to do this?).
b. Viewer sees the entire case or not at all. Would see the convicted charges along with any dismissed charges. If any charge in the case remains un-adjudicated, case will not be viewable.
c. Estimated cost is 32 hours or approximately $5,000

Option 2. Use Disposition/Judgment event codes to distinguish viewable and non-viewable events.

a. Requires separating the current sixteen Disposition/Judgment event codes into viewable or non-viewable events (advisory committee to do this?).
b. Assuming dismissed charges would be considered non-viewable and that other viewable dispositions exist (e.g., convictions), then viewer would see the case and convictions, but not any dismissed charges.
c. Estimated cost is 62 hours or approximately $10,000. Some performance impact as this requires loading of additional data upfront.

Timing: although hours are relatively low, have to work this into the budget and overall project schedule, which could take several months to accomplish. Could be done either on a phased roll out (i.e., as counties are added to MNCIS), or wait until after all counties convert to MNCIS (scheduled completion mid-2006).

Estimates do NOT include any modifications to bring online TCIS to the Internet as TCIS is being phased out by MNCIS.

MNCIS Calendar and register of actions

MNCIS has a calendar and register of actions functionality, but no estimate yet on what it might cost to implement non-searchable (e.g., PDF) format and prove-you-are-human log ins. Since it would utilize off the shelf software tools, the best guess is that the cost may be between $5,000 and $20,000 initially for the tools. How effective the tools remain over time depends on how quickly they produce updates and how quickly the hackers break them.

Concern noted by subcommittee members: if formats and log ins are too cumbersome, effective use by people is jeopardized. Consider using the invisible-to-users barriers that were used to prevent automated searches for the Hennepin property tax database.

4th District SIP (criminal)

Information presented by Jim Wehri, 4th District IT Manager:

SIP web based application in pilot/proof of concept mode (12 test users) but it does not have any security features or subscription service at this point. Developer anticipates adding these but does not have a specification and cannot estimate without a specification; also concerned about support for a subscription service. Thus subscription service for the web based application may or may not be available before 4th district fully migrates to MNCIS. Once security and subscription service are established, appears that it would be relatively easy to then modify to restrict viewing to convicted charges and eliminate active, pending cases.

SIP non-web based technology (currently implemented via subscription service) Includes any all formal charges except confidential (e.g., warrant pending) cases. Includes name search on defendant name and aliases; includes sentences and conditions, and most of what is known as a register of actions. Addresses and telephone numbers of participants included, but no SSN in SIP. Party screens (e.g., attorneys, prosecutors, defendant, probation, arresting

officer) not jurors, witnesses or victims. Includes observed race (not race census data, which is held in another database)

Change estimate: If the objective is to not show dismissed charges but show convictions only (most cases have mixtures of the two), implementing this type of rule in SIP would be extremely difficult and require 100's of hours of work as it would involve creating a different database and writing a new system to display the data. Fourth District IT would not recommend this approach because SIP will be gone in a year or two.

If the objective is to not show pre-adjudication cases, then could set up a process where cases default to a pre-adjudication status upon initiation and the default status remains until all counts are adjudicated (SIP, like MNCIS, requires each count to be adjudicated before a case can be closed). At the end of each day, the system would review all cases updated during the day to determine if adjudication has occurred on each count. If all counts are adjudicated, the classification would be changed to post-adjudication and would be viewable. Estimated that the work would be about 100 hours at a cost of approximately $8,000. There will also be considerable security and documentation work. Probably another 20 hrs.

SIP usage for each dial-up customer in February 2004: customers submitted 158,475 transactions costing $14,960.04. Money goes to general county fund intended to recover costs of SIP.

What impact on fourth district court staff if pull off pre-adjudication cases? 158,000 transactions equates to about 10,000 names being looked up. If users call the Clerks office 30% of the time to check on pre-adjudicated cases, and if it takes a clerk 5 minutes to take the call, and a clerk is available about 114 hr/mo, then the Clerk's office would need two FTE's to answer the expected calls [(10,000 x .30) x 5 min) / 60 min/hr = 250 hrs, 250/114 = 2.2 FTE's].

Impact on technology needs if pull off pre-adjudication cases? Fourth District IT expects to see an increased demand for public terminals. Public terminal costs include the initial purchase of hardware/software/furniture ($2000), network connect fee (19/mo) and transactions fees ($.0144/transaction).

User impact: Carol Buche of Tennant Check explained that her company screens approximately 1,000 rental applications a month for landlords and property managers. Pending and dismissed charges are critical to their clients. Will continue to get the pre-adjudication charges from the courts any way they can; would have to hire one more full time person just to cover fourth district courts. Not efficient to begin with arrest records from law enforcement. There

is tremendous pressure for landlords to minimize police calls to their rental property as some cities charge fees based on the level of calls. (More details on how Tennant Check operates is set forth below in the discussion on Related policy issues, assumptions, and other items).

Timing: any modifications would take staff resources away from the MNCIS implementation currently underway in the fourth district.

Experience Under 4th District subscription service: Operating since 1992. Have had some complaints; biggest issue is users not differentiating between defendant name and aliases.

Daily Calendar 4th District

Currently search by community, not by defendant name, includes main charge. Currently presented in searchable PDF format. Each calendar is available for two weeks. Estimate for producing in Image Only PDF format and using prove-you-are-human log in: 4th district has no tool currently available to perform prove you are human log in so no estimate is available. Regarding non-searchable PDF format, the calendars are produced in Power Builder and then converted to Adobe Writer, but Power Builder is unable to manipulate all of the security features in Adobe Writer to make the report Image Only. Another tool would need to be used, and although the 4th district has such a tool, the staff is not familiar with it and no estimate is available.

Related policy issues, assumptions, and other items: These items were inescapably intertwined with the subcommittee's impact assessment and discussions, and are presented as informational items to the full advisory committee.

Public terminal access at courthouse: Users will still get pre-adjudication and dismissed cases if they visit a public access terminal at the courthouse. MNCIS currently presents data only on county-by-county basis, but can be easily modified to view on a statewide basis (and current draft rule 8, subd. 2(d), which defines "remote access," permits this).

Criminal justice business partners: Current draft of rule 8, subd. 4, provides that criminal justice business partners can receive via remote or bulk any case records where access to the records in any format by such agency is authorized by law.

Searching v. Downloading or Compiling: It was noted that the current draft of rule 8, subd. 2(c), only prohibits searching by name using an automated tool

external to the courts website; it does not address plain downloading or compiling all available information in an automated fashion. That draft rule reads: "Any preconviction criminal records posted on the Internet shall be made available only by using technology which, to the extent feasible, ensures that records are not searchable by defendant name using automated tools external to the court's website." If the rule is to address automated downloading or compiling, it needs to be modified.

Subscription v. Internet: One member draws a distinction between paid subscription services and free Internet access, and would allow the former access to all cases including pre-adjudication charges, but limit the latter to post-adjudication records. Although the subscription services allow access to commercial enterprises, those enterprises presumably follow FCRA and other similar laws. If its all on the web for free, landlords will stop paying for the search and do it themselves and will not tell the applicant (as simple as not returning a phone call). In order to change the law and have the legislature require the landlord to provide reasons, use dates of birth for verification, and have current records, need court rules imposing some limitations on free Internet access; otherwise get whipsawed in the legislature, which would simply respond "but its public data from the court." Most low-income people cannot afford Internet access and shrinking library hours are further limiting their electronic access, so they have no access, regardless of what price commercial enterprises might pay for subscription services.

Other members struggled with the distinction. Some disagreed indicating that: the credit report is more important to the tenant review than the criminal record check; that the problems with web surfers and other problem users represent a tiny percentage of the overall use; and that the distinction creates a policy that is based on what a user can afford. Other members suggested a possible alternative of imposing restrictions on subscriber's use of data as part of their access to the data, although effective enforcement of such restrictions may be an issue.

Tennant Check operations: provides both a credit bureau check and a criminal records check for landlords and property managers. The cost (currently $35) is passed on to the applicant for rental. Applicant must provide a signed release (under FCRA, credit bureau will not provide the credit information without one). Landlords can reject for rental based on a felony charge as opposed to a felony conviction. Even if there are certain convictions on the record, market factors may still result in some rental property being rented.

Tennant check does not make a recommendation one way or another regarding whether to rent. Under the FCRA the landlord is required to notify the applicant if they deny rental based on the report by Tenant Check. The notice must indicate that they can get a copy of the report for free from Tennant Check within 60 days of such notice.

Under FCRA, if an applicant contests information (e.g., this particular charge or debt is not me) and Tennant Check cannot verify it, it must be removed from the report. Even if there is no correction made, the FCRA also requires a Tennant Check to include an applicant's written statement of disagreement (up to 100 words) as a part of the report.

-Mark R. Anfinson
-Sue K. Dosal
-Donald A. Gemberling
-Pamela McCabe
-Teresa Nelson
-Robert Sykora

Exhibit O: Public Hearing Witness List

Thursday, February 12, 2004
Room 230, Minnesota Judicial Center, St. Paul
(in order of appearance)

John Stuart, State Public Defender

Lucy Dalglish, Director, Reporters Committee for Freedom of the Press

Tom Johnson, Council on Crime and Justice

Pastor Albert Gallmon, Jr., Fellowship Missionary Baptist Church, Minneapolis

Archbishop Harry J. Flynn, Archdiocese of St. Paul and Minneapolis

Hon. George Stephenson, Ramsey County District Court

Prof. Jane Kirtley, Silha Center for the Study of Media Ethics and Law, School of Journalism and Mass Communication, University of Minnesota

Patricia Weinberg, Minnesota Association of Verbatim Reporters and Captioners

Gordon Stewart, Legal Rights Center

Richard Neumeister

Roger Banks, State Council on Black Minnesotans

John Borger and Chris Ison for the Star Tribune

Kizzy Johnson, Communities United Against Police Brutality

Scott Benson, Attorney and Minneapolis City Council Member

Sharon Anderson

Bishop Craig Johnson, Evangelical Lutheran Church in America

Gary Hill, KSTP TV

Exhibit P: Summary of Presentations from 2/12/04 Public Hearing

(Attached in separate file.)

Exhibit Q: Summary of Written Only Responses to Preliminary Recommendations

(Attached in separate file.)

Exhibit R: Current Access to Case Records Table

(Attached in separate file; table indicates current law and does not include proposed changes.)

Exhibit S: Current Access to Administrative Records Table

(Attached in separate file; table indicates current law and does not include proposed changes.)

Exhibit T: Current Access to Vital Statistics Records Table

(Attached in separate file; table indicates current law and does not include proposed changes.)